Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date December 9, 2021

Original Release Date August 5, 2021

Superseding Document

Status	Final
Series/Number	NIST Special Publication (SP) 800-160 Volume 2, Revision 1
Title	Developing Cyber-Resilient Systems: A Systems Security Engineering Approach
Publication Date	December 2021
DOI	https://doi.org/10.6028/NIST.SP.800-160v2r1
CSRC URL	https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final
Additional Information	Systems Security Engineering Project

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NIST Special Publication 800-160, Volume 2
Revision 1

Developing Cyber-Resilient Systems:

A Systems Security Engineering Approach

RON ROSS
VICTORIA PILLITTERI
RICHARD GRAUBART
DEBORAH BODEAU
ROSALIE MCQUAID

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-160v2r1-draft

National Institute of
Standards and Technology
U.S. Department of Commerce

Draft NIST Special Publication 800-160, Volume 2
Revision 1

Developing Cyber-Resilient Systems:

A Systems Security Engineering Approach

RON ROSS
VICTORIA PILLITTERI
Computer Security Division
National Institute of Standards and Technology

RICHARD GRAUBART
DEBORAH BODEAU
ROSALIE MCQUAID
Cyber Resiliency and Innovative
Mission Engineering Department
The MITRE Corporation
McLean, VA

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-160v2r1-draft

August 2021

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

AUTHORITY

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA), 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of the appropriate federal officials exercising policy authority over such systems. This guideline is consistent with requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, OMB Director, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-160, Vol. 2, Rev. 1
Natl. Inst. Stand. Technol. Spec. Publ. 800-160, Vol. 2, Rev. 1, **264 pages** (August 2021)

CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-160v2r1-draft

Public comment period: August 5, 2021 through September 20, 2021

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: security-engineering@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA) [FOIA96].

REPORTS ON COMPUTER SYSTEMS TECHNOLOGY

The National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology (IT). ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information systems security and privacy and its collaborative activities with industry, government, and academic organizations.

ABSTRACT

This publication is used in conjunction with ISO/IEC/IEEE 15288:2015, *Systems and software engineering—Systems life cycle processes*, NIST Special Publication (SP) 800-160, Volume 1, *Systems Security Engineering—Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, and NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations—A System Life Cycle Approach for Security and Privacy*. It can be viewed as a handbook for achieving the identified cyber resiliency outcomes based on a systems engineering perspective on system life cycle processes in conjunction with risk management processes, allowing the experience and expertise of the organization to help determine what is correct for its purpose. Organizations can select, adapt, and use some or all of the cyber resiliency constructs (i.e., objectives, techniques, approaches, and design principles) described in this publication and apply the constructs to the technical, operational, and threat environments for which systems need to be engineered.

KEYWORDS

Advanced persistent threat; controls; cyber resiliency; cyber resiliency approaches; cyber resiliency design principles; cyber resiliency engineering framework; cyber resiliency goals; cyber resiliency objectives; cyber resiliency techniques; risk management strategy; system life cycle; systems security engineering; trustworthiness.

ACKNOWLEDGMENTS

The authors gratefully acknowledge and appreciate the contributions from DJ Anand, Jon Boyens, Nicolas Chaillan, Ramaswamy Chandramouli, Ken Colerick, Ed Custeau, Holly Dunlap, David Ferraiolo, Avi Gopstein, Suzanne Hassell, Bill Heinbockel, Daryl Hild, Scott Jackson, Lauren Knausenberger, Ellen Laderman, Logan Mailloux, Jeff Marron, Cory Ocker, Rebecca Onuskanich, James Reilly, Thom Schoeffling, Martin Stanley, Shane Steiger, Mike Thomas, Beth Wilson, and David Wollman whose thoughtful comments improved the overall quality, thoroughness, and usefulness of this publication. The authors would also like to acknowledge the INCOSE Systems Security Engineering and Resiliency Working Groups, the Air Force Research Laboratory (AFRL), and the National Defense Industrial Association (NDIA) Systems Security Engineering Committee for their feedback on the initial drafts of this publication.

In addition to the above acknowledgments, a special note of thanks goes to Jeff Brewer, Jim Foti, Jeff Marron, Isabel Van Wyk, Eduardo Takamura, and the NIST web services team for their outstanding administrative support. The authors also wish to recognize the professional staff from the NIST Computer Security Division and the Applied Cybersecurity Division for their contributions in helping to improve the technical content of the publication. Finally, the authors gratefully acknowledge the significant contributions from individuals and organizations in the public and private sectors, nationally and internationally, whose insightful, thoughtful, and constructive comments improved the quality, thoroughness, and usefulness of this publication.

CYBER RESILIENCY IN THE SYSTEM LIFE CYCLE

NIST is working with the United States Air Force and the Air Force Research Laboratory (AFRL) to explore ways to incorporate the cyber resiliency constructs in this publication into the system development life cycle through the use of automated support tools. The use of such tools can help ensure that cyber resiliency requirements are clearly defined and can be more easily integrated into the system development life cycle. Automated tools can provide an efficient and effective vehicle for incorporating cyber resiliency capabilities into a variety of systems (e.g., weapons systems, space systems, command and control systems, industrial control systems, enterprise IT systems) using any established life cycle development process or approach (e.g., agile, waterfall, spiral, DevOps). Automation can also support the rapid testing and evaluation of cyber resiliency capabilities in critical systems to reduce the time to operational deployment.

NOTES TO REVIEWERS

This update constitutes the first revision to NIST Special Publication (SP) 800-160, Volume 2. In addition to a general review and update of the entire publication, there are five significant changes that either add new content or move current content to a new location. These include:

1. Updating the controls that support cyber resiliency to be consistent with NIST SP 800-53, Revision 5 [SP 800-53]
2. Standardizing on a single threat taxonomy (i.e., Adversarial Tactics, Techniques, and Common Knowledge [ATT&CK] framework) [MITRE18]
3. Providing a detailed mapping and analysis of the cyber resiliency implementation approaches and supporting controls to the ATT&CK framework techniques, mitigations, and candidate mitigations
4. Eliminating Appendix F on *Cyber Resiliency in the System Life Cycle* which will be reflected in the update to NIST SP 800-160, Volume 1 [SP 800-160 v1]
5. Moving cyber resiliency use cases and examples in Appendices I and J to the NIST SP 800-160, Volume 2 website at https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final (available upon final publication)

Your feedback on this draft publication is important to us. We appreciate each contribution from our reviewers. The very insightful comments from both the public and private sectors, nationally and internationally, continue to help shape the final publication to ensure that it meets the needs and expectations of our customers.

CALL FOR PATENT CLAIMS

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i) under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii) without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: security-engineering@nist.gov.

EXECUTIVE SUMMARY

The goal of the NIST Systems Security Engineering initiative is to address security, safety, and resiliency issues from the perspective of stakeholder requirements and protection needs using established engineering processes to ensure that those requirements and needs are addressed across the entire system life cycle to develop more trustworthy systems.[1] To that end, NIST Special Publication (SP) 800-160, Volume 2, focuses on cyber resiliency engineering—an emerging specialty systems engineering discipline applied in conjunction with resilience engineering and systems security engineering to develop more survivable, trustworthy systems. Cyber resiliency engineering intends to architect, design, develop, maintain, and sustain the trustworthiness of systems with the capability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises that use or are enabled by cyber resources. From a risk management perspective, cyber resiliency is intended to reduce the mission, business, organizational, or sector risk of depending on cyber resources.

This publication is intended to be used in conjunction with ISO/IEC/IEEE 15288:2015, *Systems and software engineering—Systems life cycle processes*; NIST SP 800-160, Volume 1, *Systems Security Engineering—Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*; and NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations—A System Life Cycle Approach for Security and Privacy*. The application of the principles in this publication—in combination with the system life cycle processes in SP 800-160, Volume 1, and the risk management methodology in SP 800-37—can be viewed as a handbook for achieving cyber resiliency outcomes. Guided and informed by stakeholder protection needs, mission and business assurance needs, and stakeholder concerns with cost, schedule, and performance, the cyber resiliency constructs, principles, and analysis methods can be applied to critical systems to identify, prioritize, and implement solutions to meet the unique cyber resiliency needs of organizations.

NIST SP 800-160, Volume 2, presents a cyber resiliency engineering framework to help aid in understanding and applying cyber resiliency, a concept of use for the framework, and the engineering considerations for implementing cyber resiliency in the system life cycle. The cyber resiliency engineering framework constructs include goals, objectives, techniques, approaches, and design principles. Organizations can select, adapt, and use some or all of the cyber resiliency constructs in this publication and apply the constructs to the technical, operational, and threat environments for which systems need to be engineered.

Building off of the cyber resiliency engineering framework, this publication also identifies considerations for determining which cyber resiliency constructs are most relevant to a system-of-interest and a tailorable cyber resiliency analysis approach to apply the cyber resiliency concepts, constructs, and practices to a system. The cyber resiliency analysis is intended to determine whether the cyber resiliency properties and behaviors of a system-of-interest,

[1] In the context of systems engineering, trustworthiness means being trusted to fulfill whatever critical requirements may be needed for a particular component, subsystem, system, network, application, mission, enterprise, or other entity. Trustworthiness requirements can include attributes of safety, security, reliability, dependability, performance, resilience, and survivability under a wide range of potential adversity in the form of disruptions, hazards, and threats [SP 800-160 v1].

wherever it is in the life cycle, are sufficient for the organization using that system to meet its mission assurance, business continuity, or other security requirements in a threat environment that includes the advanced persistent threat (APT). A cyber resiliency analysis is performed with the expectation that such analysis will support engineering and risk management decisions about the system-of-interest.

The cyber resiliency engineering framework is supplemented by several technical appendices that provide additional information to support its application, including:

- Background and contextual information on cyber resiliency
- Detailed descriptions of the individual cyber resiliency constructs (i.e., goals, objectives, techniques, implementation approaches, design principles) that are part of the cyber resiliency engineering framework
- Controls in [SP 800-53] which directly support cyber resiliency (including the questions used to determine if controls support cyber resiliency, the relevant controls, and resiliency techniques and approaches)
- An approach for adversary-oriented analysis of a system and applications of cyber resiliency, a vocabulary to describe the current or potential effects of a set of mitigations, and a representative analysis of how cyber resiliency approaches and controls could mitigate adversary tactics, techniques, and procedures.

TABLE OF CONTENTS

DISCLAIMER

This publication is intended to be used in conjunction with and as a supplement to **International Standard ISO/IEC/IEEE 15288**, *Systems and software engineering — System life cycle processes*. It is strongly recommended that organizations using this publication obtain the standard in order to fully understand the context of the security-related activities and tasks in each of the system life cycle processes. Content from the international standard that is referenced in this publication is used with permission from the Institute of Electrical and Electronics Engineers and is noted as follows:

[**ISO 15288**]. *Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.*

241

RELATIONSHIP BETWEEN ISO 15288 AND OPERATIONAL RESILIENCE

Alhough the focus of [ISO 15288] is the systems and software engineering processes, operational resilience, which includes cyber resiliency for systems that include or depend on cyber resources, is addressed indirectly by requiring organization-wide commitment, resources, practices, and processes. The interacting elements in the definition of a *system* include layers of resilience in hardware, software, data, information, humans, processes, procedures, facilities, materials, and naturally occurring physical entities. This is important because if the organization's missions or business functions require sustainability during perturbations, disruptions, disturbances, or cyber attacks, then operational resilience practices and procedures must be applied to all of the system's assets. It would be of limited value to have resilience measures implemented in the software architecture if there is no redundancy and survivability in the hardware, if the communications networks are fragile, if critical personnel are not available (e.g., in a natural disaster or inclement weather) to operate and maintain the system, or if there are no facilities available for producing the organization's products and/or services.

SYSTEM RESILIENCE AND CYBER RESILIENCY

This publication focuses on cyber resiliency engineering as a specialty systems engineering discipline applied in conjunction with resilience engineering and systems security engineering. The relationship between these disciplines can be seen in the example of an automobile. An automobile contains many cyber resources including embedded control units for acceleration, braking, and engine control as well as entertainment and cellular communications systems. The automobile and its human operators can be viewed as a *system-of-interest* from the systems security engineering perspective as described in [SP 800-160 v1]. The system-of-interest has an assumed environment of operation (including the countries in which the vehicle is sold), which includes assumptions about the distribution of fuel or charging stations.

As a system element, the fuel or battery system includes cyber resources (e.g., to perform fuel consumption or battery use analysis and predict the remaining travel range). A *system resilience engineering analysis*—an analysis of the resilience of the system-of-interest to predictable, disruptive, or destructive events, due to accidents, structural failure, or human error—considers whether and how easily the operator could fail to notice a low-fuel or low-battery indicator. In addition, a system resilience (or system resiliency) engineering analysis considers whether the expected travel range of the vehicle is shorter than the expected maximum distance between fuel or charging stations in the intended operational environment.

A *cyber resiliency engineering analysis* of the fuel or battery system considers ways in which false information about the fuel level could be presented to the operator or to other system elements (e.g., an engine fail-safe which cuts off or deactivates if no fuel is being supplied) because of malware introduced into fuel consumption analysis. A cyber resiliency engineering analysis also considers ways in which other system elements could detect or compensate for the resulting misbehavior or prevent the malware from being introduced. While such an analysis could be made part of a general system resilience engineering analysis, it requires specialized expertise about how the APT can find and exploit vulnerabilities in the cyber resources, as well as about techniques that could be used to reduce the associated risks.

244

ADVERSARY PERSISTENCE AND LONG-TERM PRESENCE

Numerous reports of cyber incidents and cyber breaches indicate that extended periods of time transpired between the time an adversary initially established a presence in an organizational system by exploiting a vulnerability and when that presence was revealed or detected. In certain instances, the time periods before detection can be as longs as months or years. In the worst case, the adversary's presence may never be detected.

The following examples illustrate the types of situations where an adversary can maintain a long-term presence or persistence in a system, even without attacking the system via cyberspace:

- Compromising the *pre-execution environment* of a system through a hardware or software implant (e.g., compromise of the firmware or microcode of a system element, such as a network switch or a router, that activates before initialization in the system's environment of operation). This is extremely difficult to detect and can result in compromise of the entire environment.
- Compromising the *software development tool-chain* (e.g., compilers, linkers, interpreters, continuous integration tools, code repositories). This allows malicious code to be inserted by the adversary without modifying the source code or without the knowledge of the software developers.
- Compromising a *semiconductor product or process* (e.g., malicious alteration to the hardware description language [HDL] of a microprocessor, a field-programmable gate array [FPGA], a digital signal processor [DSP], or an application-specific integrated circuit [ASIC]).

245

THREAT DETECTION AND CYBER RESILIENCY

Cyber resiliency is based on the recognition that adversaries can establish and maintain a covert presence in systems. Therefore, many of the cyber resiliency techniques and approaches are not predicated on the assumption of successfully detecting adversity including cyber attacks. These include the Coordinated Protection, Deception, Diversity, Non-Persistence, Realignment, Redundancy, Substantiated Integrity, and Unpredictability techniques, and the Fragmentation, Distributed Functionality, Predefined Segmentation, Attribute-Based Usage Restriction, and Trust-Based Privilege Management approaches.

Other techniques and approaches can provide automatic response—or can support cyber defender responses—to detected indicators of possible or suspected adversity, or to warnings of potential forthcoming adverse conditions (including predictions of increased system load or announcements of planned outages of supporting services). These include the Adaptive Response technique and the Functional Relocation of Sensors, Functional Relocation of Cyber Resources, Asset Mobility, Dynamic Privileges, and Dynamic Segmentation and Isolation approaches.

Two cyber resiliency techniques directly involve the detection of adversity or its effects: These include Analytic Monitoring and Contextual Awareness. The Substantiated Integrity technique and the Consistency Analysis approach support detection of some effects of adversity.

ERRATA

This table contains changes that have been incorporated into Special Publication 800-160, Volume 2, Revision 1. Errata updates can include corrections, clarifications, or other minor changes in the publication that are either *editorial* or *substantive* in nature. Any potential updates for this document that are not yet published in an errata update or revision—including additional issues and potential corrections—will be posted as they are identified; see the SP 800-160 Volume 2, Revision 1 publication details.

DATE	TYPE	REVISION	PAGE

PROLOGUE

"If a full on 'turn the lights off' cyber war were to happen today, we would lose. Think about that. We would lose a cyber war. With a few clicks of the mouse, and in just a few seconds, hackers … could turn off our electricity, millions would lose heat, groceries would spoil, banking machines would not work, and people could not get gasoline. It would be what we have seen down in Texas, but on national scale and with no end in sight. That we have escaped a digital catastrophe thus far is not due to skill. It is due to blind luck and restraint from our adversaries."

Mike Rogers, February 2021
Former Member of Congress, House Intelligence Committee

"Providing satisfactory security controls in a computer system is in itself a system design problem. A combination of hardware, software, communications, physical, personnel and administrative-procedural safeguards is required for comprehensive security. In particular, software safeguards alone are not sufficient."

The Ware Report
Defense Science Board Task Force on Computer Security, 1970.

"This whole economic boom in cybersecurity seems largely to be a consequence of poor engineering."

Carl Landwehr
Communications of the ACM, February 2015

"Mission assurance requires systems that behave with predictability and proportionality."

General Michael Hayden
Former NSA and CIA Director, Syracuse University, October 2009

"In the past, it has been assumed that to show that a system is safe, it is sufficient to provide assurance that the process for identifying the hazards has been as comprehensive as possible, and that each identified hazard has one or more associated controls."

While historically this approach has been used reasonably effectively to ensure that known risks are controlled, it has become increasingly apparent that evolution to a more holistic approach is needed as systems become more complex and the cost of designing, building, and operating them become more of an issue."

Preface, NASA Systems Safety Handbook, Volume 1

CHAPTER ONE

INTRODUCTION

THE NEED FOR CYBER-RESILIENT SYSTEMS

The need for trustworthy secure *systems*[2] stems from a variety of *stakeholder* needs that are driven by mission, business, and other objectives and concerns. The principles, concepts, and practices for engineering trustworthy secure systems can be expressed in various ways, depending on which aspect of trustworthiness is of concern to stakeholders. NIST Special Publication (SP) 800-160, Volume 1 [SP 800-160 v1], provides guidance on systems security engineering with an emphasis on protection against *asset* loss.[3] In addition to security, other aspects of trustworthiness include reliability, safety, and resilience. Specialty engineering disciplines address different aspects of trustworthiness. While each discipline frames the problem domain and the potential solution space for its aspect of trustworthiness somewhat differently, [SP 800-160 v1] includes systems engineering processes to align the concepts, frameworks, and analytic processes from multiple disciplines to make trade-offs within and between the various aspects of trustworthiness applicable to a *system-of-interest*.[4]

NIST SP 800-160, Volume 2, focuses on the property of *cyber resiliency*, which has a strong relationship to security and resilience but which provides a distinctive framework for its identified problem domain and solution space. Cyber resiliency is 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.[5]

Cyber resiliency can be sought at multiple levels, including for system elements, systems, missions or business functions and the system-of-systems which support those functions, organizations, sectors, regions, the Nation, or transnational missions/business functions. From an engineering perspective, cyber resiliency is an emergent quality property of an engineered system, where an "engineered system" can be a system element made up of constituent components, a system, or a system-of-systems. Cyber-resilient systems are those systems that have security measures or safeguards "built in" as a foundational part of the architecture and design and that display a high level of resiliency. Thus, cyber-resilient systems can withstand cyber attacks, faults, and failures and continue to operate in a degraded or debilitated state to

[2] A *system* is a combination of interacting elements organized to achieve one or more stated purpose. The interacting system elements that compose a system include hardware, software, data, humans, processes, procedures, facilities, materials, and naturally occurring entities [ISO 15288].

[3] An *asset* refers to an item of value to stakeholders. Assets may be tangible (e.g., a physical item, such as hardware, firmware, computing platform, network device, or other technology component, or individuals in key or defined roles in organizations) or intangible (e.g., data, information, software, trademark, copyright, patent, intellectual property, image, or reputation). Refer to [SP 800-160 v1] for the systems security engineering perspective on assets.

[4] A *system-of-interest* is a system whose life cycle is under consideration in the context of [ISO 15288]. A system-of-interest can also be viewed as the system that is the focus of the systems engineering effort. The system-of-interest contains system elements, system element interconnections, and the environment in which they are placed.

[5] The term *adversity* is used in this publication to mean adverse conditions, stresses, attacks, or compromises and is consistent with the use of the term in [SP 800-160 v1] as disruptions, hazards, and threats. Adversity in the context of the definition of cyber resiliency specifically includes but is not limited to cyber attacks. For example, cyber resiliency engineering analysis considers the potential consequences of physical destruction of a cyber resource to the system-of-interest of which that resource is a system element.

carry out the mission-essential functions of the organization. From an enterprise risk management perspective, cyber resiliency is intended to reduce the mission, business, organizational, or sector risk of depending on cyber resources.

Cyber resiliency supports mission assurance in a contested environment for missions that depend on systems which include cyber resources. A *cyber resource* is an information resource which creates, stores, processes, manages, transmits, or disposes of information in electronic form and which can be accessed via a network or using networking methods. However, some information resources are specifically designed to be accessed using a networking method only intermittently (e.g., via a low-power connection to check the status of an insulin pump, via a wired connection to upgrade software in an embedded avionic device). These cyber resources are characterized as operating primarily in a disconnected or non-networked mode.[6]

CYBER-RESILIENT SYSTEMS

Cyber-resilient systems operate somewhat like the human body. The human body has a powerful immune system that absorbs a constant barrage of environmental hazards and provides the necessary defense mechanisms to maintain a healthy state. The human body also has self-repair systems to recover from illnesses and injuries when defenses are breached. But cyber-resilient systems, like the human body, cannot defend against all hazards at all times. While the body cannot always recover to the same state of health as before an injury or illness, it can adapt. Similarly, cyber-resilient systems can recover minimal essential functionality. Understanding the limitations of individuals, organizations, and engineered systems is fundamental to managing risk.

Systems increasingly incorporate cyber resources as *system elements*. As a result, systems are susceptible to harms resulting from the effects of adversity on cyber resources and particularly to harms resulting from cyber attacks. The cyber resiliency problem is defined as how to achieve adequate mission resilience by providing (1) adequate *system resilience*[7] and (2) adequate mission/business function and operational/organizational resilience in the presence of possible adversities that affect cyber resources. The cyber resiliency problem domain overlaps with the security problem domain since a system should be *securely resilient*.[8] The cyber resiliency problem domain is guided and informed by an understanding of the threat landscape and, in particular, the *advanced persistent threat* (APT). The APT is an adversary that possesses significant levels of expertise and resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors, including cyber, physical, and deception. These objectives typically include establishing and extending footholds within the systems of the

[6] Some information resources, which include computing hardware, software, and stored information, are designed to be inaccessible via networking methods but can be manipulated physically or electronically to yield information or to change behavior (e.g., side-channel attacks on embedded cryptographic hardware). Such system elements may also be considered cyber resources for the purposes of cyber resiliency engineering analysis.

[7] *System resilience* is defined by the INCOSE Resilient Systems Working Group (RSWG) as "the capability of a system with specific characteristics before, during, and after a disruption to absorb the disruption, recover to an acceptable level of performance, and sustain that level for an acceptable period of time [INCOSE11]."

[8] The term *securely resilient* refers to the system's ability to preserve a secure state despite disruption, including the system transitions between normal and degraded modes. A primary objective of systems security engineering [SP 800-160 v1] is ensuring that the system is securely resilient.

targeted organizations for the express purposes of exfiltrating information; undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The APT pursues its objectives repeatedly over an extended period, adapts to defenders' efforts to resist it, and is determined to maintain the level of interaction needed to execute its objectives [SP 800-39] [CNSSI 4009].[9]

All discussions of cyber resiliency focus on assuring mission or business functions and are predicated on the assumption that the adversary will breach defenses and establish a long-term presence in organizational systems. A *cyber-resilient system* is a system that provides a degree of cyber resiliency commensurate with the system's criticality. It treats cyber resiliency as one aspect of trustworthiness that requires assurance in conjunction with other aspects, such as security, reliability, and safety.

1.1 PURPOSE AND APPLICABILITY

The purpose of this document is to supplement [SP 800-160 v1] and [SP 800-37] (or other risk management processes or methodologies) with guidance on how to apply cyber resiliency concepts, constructs, and engineering practices as part of systems security engineering and risk management for systems and organizations. This document identifies considerations of the engineering of systems that include the following circumstances or systems that depend on cyber resources. Circumstances or types of systems to which this document applies include:[10]

- **Circumstances:** New systems, reactive modifications to fielded systems, planned upgrades to fielded systems while continuing to sustain day-to-day operations, evolution of systems, and retirement of systems
- **Types of systems:**
  - General-purpose or multi-use systems (e.g., enterprise information technology [EIT]), shared services, or common infrastructures
  - Dedicated or special-purpose systems (e.g., security-dedicated or security-purposed systems, cyber-physical systems [CPS],[11] Internet of Things [IoT], or Network of Things [NoT][12])
  - Large-scale processing environments
  - Systems-of-systems (e.g., critical infrastructure systems [CIS])

[9] While some sources define the APT to be an adversary at Tier V or Tier VI in the threat model in [DSB13], in particular, to be a state actor, the definition used in this publication includes any actors with the characteristics described above. The above definition also includes adversaries that subvert the supply chain to compromise cyber resources, which are subsequently made part of the system-of-interest. As discussed in Chapter Two and Section D.2, the APT is a crucial aspect of the threat landscape for cyber resiliency engineering.

[10] This list is not intended to be exhaustive or mutually exclusive. Circumstances and types of systems are discussed in more detail in Section 2.2 and Section 3.1.3.

[11] A cyber-physical system (CPS) is a system that includes engineered interacting networks of computational and physical components. CPSs range from simple devices to complex systems-of-systems. A CPS device is a device that has an element of computation and interacts with the physical world through sensing and actuation [SP 1500-201].

[12] A Network of Things (NoT) is a system consisting of devices that include a sensor and a communications capability, a network, software that aggregates sensor data, and an external utility (i.e., a software or hardware product or service that executes processes or feeds data into the system) [SP 800-183].

1.2 TARGET AUDIENCE

This publication is intended for systems security engineering and other professionals who are responsible for the activities and tasks related to the system life cycle processes in [SP 800-160 v1], the risk management processes in [SP 800-39], or the Risk Management Framework (RMF) in [SP 800-37].[13] The term *systems security engineer* is used in this publication to include those security professionals who perform any of the activities and tasks in [SP 800-160 v1]. This publication can also be used by professionals who perform other system life cycle activities that impact trustworthiness or who perform activities related to the education or training of systems engineers and systems security engineers. These include but are not limited to:

- Individuals with systems engineering, architecture, design, development, and integration responsibilities
- Individuals with software engineering, architecture, design, development, integration, and software maintenance responsibilities
- Individuals with security governance, risk management, and oversight responsibilities, particularly those defined in [SP 800-37]
- Individuals with independent security verification, validation, testing, evaluation, auditing, assessment, inspection, and monitoring responsibilities
- Individuals with system security administration, operations, maintenance, sustainment, logistics, and support responsibilities
- Individuals with acquisition, budgeting, and project management responsibilities;
- Providers of technology products, systems, or services
- Academic institutions offering systems security engineering and related programs

This publication assumes that the systems security engineering activities in [SP 800-160 v1] and risk management processes in [SP 800-37] are performed under the auspices of or within an organization (referred to as "the organization" in this document).[14] The activities and processes take into consideration the concerns of a variety of stakeholders, within and external to the organization. The organization—through systems security engineering and risk management activities—identifies stakeholders, elicits their concerns, and represents those concerns in the systems security engineering and risk management activities.

1.3 HOW TO USE THIS PUBLICATION

This publication is intended to be used in conjunction with [SP 800-160 v1] and is designed to be flexible in its application to meet the diverse and changing needs of organizations. It is not intended to provide a specific recipe for execution. Rather, the publication can be viewed as a catalog or handbook for achieving the identified cyber resiliency outcomes from a systems

[13] This includes security and risk management practitioners with significant responsibilities for the protection of existing systems, information, and the information technology infrastructure within enterprises (i.e., the installed base). Such practitioners may use the cyber resiliency content in this publication in other than engineering-based system life cycle processes. These application areas may include use of the *Risk Management Framework* [SP 800-37], the controls in [SP 800-53], or the *Framework for Improving Critical Infrastructure Cybersecurity* [NIST CSF] where such applications have cyber resiliency-related concerns.

[14] Systems security engineering and risk management apply to systems-of-systems in which multiple organizations are responsible for constituent systems. In such situations, systems security engineering and risk management activities are performed within individual organizations (each an instance of "the organization") and supported by cooperation or coordination across those organizations.

engineering perspective on system life cycle processes, leveraging the experience and expertise of the engineering organization to determine what is correct for its purpose. Stakeholders choosing to use this guidance can employ some or all of the cyber resiliency constructs (i.e., goals, objectives, techniques, approaches, and design principles) as well as the analytic and life cycle processes, tailoring them to the technical, operational, and threat environments for which systems need to be engineered. In addition, organizations choosing to use this guidance for their systems security engineering efforts can select and employ some or all of the thirty processes in [ISO 15288] and some or all of the security-related activities and tasks defined for each process. Note that there are process dependencies in [ISO 15288]. The successful completion of some activities and tasks invokes other processes or leverages the results of other processes.

The system life cycle processes can be used for new systems, system upgrades, or systems that are being repurposed. The processes can be employed at any stage of the system life cycle and can take advantage of any system or software development methodology, including waterfall, spiral, or agile. The life cycle processes can also be applied recursively, iteratively, concurrently, sequentially, or in parallel and to any system regardless of its size, complexity, purpose, scope, environment of operation, or special nature.

The full extent of the application of the content in this publication is informed by stakeholder needs, organizational capability, and cyber resiliency goals and objectives, as well as concerns for cost, schedule, and performance. The tailorable nature of the engineering activities and tasks and the system life cycle processes help to ensure that the specific systems resulting from the application of the security design principles and concepts have a level of trustworthiness deemed sufficient to protect stakeholders from suffering unacceptable losses of assets and the associated consequences. Such trustworthiness is made possible by the rigorous application of those cyber resiliency design principles, constructs, and concepts within a structured set of processes that provides the necessary evidence and transparency to support risk-informed decision making and trades.

1.4 PUBLICATION ORGANIZATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the framework for cyber resiliency engineering.
- **Chapter Three** describes considerations for selecting and prioritizing cyber resiliency techniques and implementation approaches and presents a tailorable process for applying cyber resiliency concepts, constructs, and practices to a system.

The following sections provide additional cyber resiliency-related information, including:

- **References**[15]
- **Appendix A**: Glossary
- **Appendix B**: Acronyms
- **Appendix C**: Background
- **Appendix D**: Cyber Resiliency Constructs

[15] Unless otherwise stated, all references to NIST publications refer to the most recent version of those publications.

439 • **Appendix E**: Controls Supporting Cyber Resiliency
440 • **Appendix F**: Adversary-Oriented Analysis
441
442

CYBER RESILIENCY—A NECESSARY SYSTEM PROPERTY

Most engineered systems incorporate or depend on cyber resources and are therefore, highly susceptible to adversity that affects such resources and particularly to cyber attacks. Harms resulting from cyber attacks and the effects of faults, failures, and human errors—which adversaries can leverage and emulate—are experienced at the organizational level, mission or business process level, and the system level [SP 800-39]. The management of cyber risks is thus an increasingly crucial aspect of any risk management program.

Cyber resiliency is defined 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." (See Section C.1 for additional information on how this definition relates to other resilience-related definitions.) Systems with this property are characterized by security measures that are "built in" as a foundational part of the architecture and design. Moreover, these systems can withstand cyber attacks, faults, and failures and can continue to operate even in a degraded or debilitated state, carrying out mission-essential functions, and ensuring that the other aspects of trustworthiness (i.e., safety and information security) are preserved.

Cyber resiliency must be provided in a cyber-contested environment that includes the Advanced Persistent Threat (APT). Therefore, any discussion of cyber resiliency is predicated on the assumption that adversaries will breach defenses and that, whether via breaches or via supply chain attacks, adversaries will establish a long-term presence in organizational systems. (See Section C.2 for more information on the characteristics of cyber resiliency.) The assumption of a sophisticated, well-resourced, and persistent adversary whose presence in systems can go undetected for extended periods is a key differentiator between cyber resiliency and other aspects of trustworthiness.

443

CHAPTER TWO

THE FUNDAMENTALS

UNDERSTANDING THE CONCEPTS ASSOCIATED WITH CYBER RESILIENCY

This section presents an engineering framework for understanding and applying cyber resiliency, the cyber resiliency constructs that are part of the framework, a concept of use for the framework, and engineering considerations for implementing cyber resiliency in the system life cycle. The discussion relies on several terms including cyber resiliency concepts, constructs, engineering practices, and solutions.

Cyber resiliency *concepts* are related to the problem domain and the solution set for cyber resiliency. The concepts are represented in cyber resiliency risk models and by cyber resiliency constructs.[16] The *constructs* are the basic elements (i.e., building blocks) of the cyber resiliency engineering framework and include goals, objectives, techniques, implementation approaches, and design principles.[17] The framework provides a way to understand the cyber resiliency problem and solution domain. Cyber resiliency goals and objectives identify the "what" of cyber resiliency—that is, what properties and behaviors are integral to cyber-resilient systems. Cyber resiliency techniques, implementation approaches, and design principles characterize the ways of achieving or improving resilience in the face of threats to systems and system components (i.e., the "how" of cyber resiliency). Cyber resiliency constructs address both adversarial and non-adversarial threats from cyber and non-cyber sources. The concern for cyber resiliency focuses on aspects of trustworthiness—in particular, security and resilience—and risk from the perspective of mission assurance against determined adversaries (e.g., the APT).

Cyber resiliency *engineering practices* are the methods, processes, modeling, and analytical techniques used to identify and analyze proposed cyber resiliency solutions. The application of cyber resiliency engineering practices in system life cycle processes ensures that cyber resiliency *solutions* are driven by stakeholder requirements and protection needs, which, in turn, guide and inform the development of system requirements for the system-of-interest [ISO 15288, SP 800-160 v1]. Such solutions consist of combinations of technologies, architectural decisions, systems engineering processes, and operational policies, processes, procedures, or practices that solve problems in the cyber resiliency domain. That is, they provide a sufficient level of cyber resiliency to meet stakeholder needs and reduce risks to organizational mission or business capabilities in the presence of a variety of threat sources, including the APT.

Cyber resiliency *solutions* use cyber resiliency techniques and approaches to implementing those techniques, as described in Section 2.1.3. Cyber resiliency solutions apply the design principles described in Section 2.1.4. Cyber resiliency solutions typically implement mechanisms (e.g., controls and control enhancements defined in [SP 800-53]) that apply one or more cyber resiliency techniques or implementation approaches or that are intended to achieve one or more cyber resiliency objectives. These mechanisms are selected in response to the security and cyber resiliency requirements defined as part of the system life cycle requirements engineering

[16] As discussed in Section D.1, cyber resiliency concepts and constructs are informed by definitions and frameworks related to other forms of resilience as well as system survivability. A reader unfamiliar with the concept of resilience may benefit from reading that appendix before this section.

[17] Additional constructs (e.g., sub-objectives, capabilities) may be used in some modeling and analytic practices.

process described in [SP 800-160 v1] or to mitigate security and cyber resiliency risks that arise from architectural or design decisions.

2.1 CYBER RESILIENCY ENGINEERING FRAMEWORK

The following sections provide a description of the framework for cyber resiliency engineering.[18] The framework constructs include cyber resiliency goals, objectives, techniques, approaches, and design principles. The relationship among constructs is also described. These constructs, like cyber resiliency, can be applied at levels beyond the system (e.g., mission or business function level, organizational level, or sector level). Table 1 summarizes the definition and purpose of each construct and how each construct is applied at the system level.

TABLE 1: CYBER RESILIENCY CONSTRUCTS

CONSTRUCT	DEFINITION, PURPOSE, AND APPLICATION AT THE SYSTEM LEVEL
GOAL	A high-level statement supporting (or focusing on) one aspect (i.e., anticipate, withstand, recover, adapt) in the definition of cyber resiliency.
	Purpose: Align the definition of cyber resiliency with definitions of other types of resilience. **Application:** Can be used to express high-level stakeholder concerns, goals, or priorities.
OBJECTIVE	A high-level statement (designed to be restated in system-specific and stakeholder-specific terms) of what a system must achieve in its operational environment and throughout its life cycle to meet stakeholder needs for mission assurance and resilient security; the objectives are more specific than goals and more relatable to threats.
	Purpose: Enable stakeholders and systems engineers to reach a common understanding of cyber resiliency concerns and priorities; facilitate the definition of metrics or measures of effectiveness (MOEs). **Application:** Used in scoring methods or summaries of analyses (e.g., cyber resiliency posture assessments).
Sub-Objective	A statement, subsidiary to a cyber resiliency objective, which emphasizes different aspects of that objective or identifies methods to achieve that objective.
	Purpose: Serve as a step in the hierarchical refinement of an objective into activities or capabilities for which performance measures can be defined. **Application:** Used in scoring methods or analyses; may be reflected in system functional requirements.
Activity or Capability	A statement of a capability or action which supports the achievement of a sub-objective and, hence, an objective.
	Purpose: Facilitate the definition of metrics or MOEs. While a representative set of activities or capabilities have been identified in [Bodeau18b], these are intended solely as a starting point for selection, tailoring, and prioritization. **Application:** Used in scoring methods or analyses; reflected in system functional requirements.
STRATEGIC DESIGN PRINCIPLE	A high-level statement which reflects an aspect of the risk management strategy that informs systems security engineering practices for an organization, mission, or system.

[18] The cyber resiliency engineering framework described in this publication is based on and consistent with the *Cyber Resiliency Engineering Framework* developed by The MITRE Corporation [Bodeau11].

CONSTRUCT	DEFINITION, PURPOSE, AND APPLICATION AT THE SYSTEM LEVEL
	Purpose: Guide and inform engineering analyses and risk analyses throughout the system life cycle. Highlight different structural design principles, cyber resiliency techniques, and implementation approaches. **Application:** Included, cited, or restated in system non-functional requirements (e.g., requirements in a Statement of Work [SOW] for analyses or documentation).
STRUCTURAL DESIGN PRINCIPLE	A statement which captures experience in defining system architectures and designs.
	Purpose: Guide and inform design and implementation decisions throughout the system life cycle. Highlight different cyber resiliency techniques and implementation approaches. **Application:** Included, cited, or restated in system non-functional requirements (e.g., Statement of Work [SOW] requirements for analyses or documentation); used in systems engineering to guide the use of techniques, implementation approaches, technologies, and practices.
TECHNIQUE	A set or class of technologies, processes, or practices providing capabilities to achieve one or more cyber resiliency objectives.
	Purpose: Characterize technologies, practices, products, controls, or requirements so that their contribution to cyber resiliency can be understood. **Application:** Used in engineering analysis to screen technologies, practices, products, controls, solutions, or requirements; used in the system by implementing or integrating technologies, practices, products, or solutions.
IMPLEMENTATION APPROACH	A subset of the technologies and processes of a cyber resiliency technique, defined by how the capabilities are implemented.
	Purpose: Characterize technologies, practices, products, controls, or requirements so that their contribution to cyber resiliency and their potential effects on threat events can be understood. **Application:** Used in engineering analysis to screen technologies, practices, products, controls, solutions, or requirements; used in the system by implementing or integrating technologies, practices, products, or solutions.
SOLUTION	A combination of technologies, architectural decisions, systems engineering processes, and operational processes, procedures, or practices that solves a problem in the cyber resiliency domain.
	Purpose: Provide a sufficient level of cyber resiliency to meet stakeholder needs and reduce risks to mission or business capabilities in the presence of advanced persistent threats. **Application:** Integrated into the system or its operational environment.
MITIGATION	An action or practice, using a technology, control, solution, or a set of these, that reduces the level of risk associated with a threat event or threat scenario.
	Purpose: Characterize actions, practices, approaches, controls, solutions, or combinations of these in terms of their potential effects on threat events, threat scenarios, or risks. **Application:** Integrated into the system as it is used.

2.1.1 Cyber Resiliency Goals

Cyber resiliency, like security, is a concern at multiple levels in an organization. The four cyber resiliency goals, which are common to many resilience definitions, are included in the definition and the cyber resiliency engineering framework to provide linkage between risk management decisions at the mission and business process level and at the system level with those at the

498 organizational level. Organizational risk management strategies can use the cyber resiliency
499 goals and associated strategies to incorporate cyber resiliency.[19]

500 For cyber resiliency engineering analysis, cyber resiliency objectives[20] rather than goals are the
501 starting point. The term *adversity*, as used in the cyber resiliency goals in Table 2, includes
502 stealthy, persistent, sophisticated, and well-resourced adversaries (i.e., the APT) who may have
503 compromised system components and established a foothold within an organization's systems.

504 **TABLE 2: CYBER RESILIENCY GOALS**

GOAL	DESCRIPTION
ANTICIPATE	Maintain a state of informed preparedness for adversity.
	Discussion: Adversity refers to adverse conditions, stresses, attacks, or compromises on cyber resources. Adverse conditions can include natural disasters and structural failures (e.g., power failures). Stresses can include unexpectedly high-performance loads. Adversity can be caused or taken advantage of by an APT actor. Informed preparedness involves contingency planning, including plans for mitigating attacks as well as for responding to discoveries of vulnerabilities or supply chain compromises. Cyber threat intelligence (CTI) provides vital information for informed preparedness.
WITHSTAND	Continue essential mission or business functions despite adversity.
	Discussion: Detection is not required for this goal to be meaningful and achievable. An APT actor's activities may be undetected, or they may be detected but incorrectly attributed to user error or other stresses. Identification of essential organizational missions or business functions is necessary to achieve this goal. In addition, supporting processes, systems, services, networks, and infrastructures must also be identified. The criticality of resources and capabilities of essential functions can vary over time.
RECOVER	Restore mission or business functions during and after adversity.
	Discussion: The restoration of functions (including data) can be incremental. A key challenge is to determine how much trust can be placed in restored functions and data as restoration progresses. Other threat events or conditions in the operational or technical environment can interfere with recovery, and an APT actor may seek to take advantage of confusion about recovery processes to establish a new foothold in the organization's systems.
ADAPT	Modify mission or business functions and/or supporting capabilities in response to predicted changes in the technical, operational, or threat environments.
	Discussion: Change can occur at different scales and over different time frames, so tactical and strategic adaption may be needed. Modification can be applied to processes and procedures as well as technology. Changes in the technical environment can include emerging technologies (e.g., artificial intelligence, 5G, Internet of Things) as well as the retirement of obsolete products. Changes in the operational environment of the organization can result from regulatory or policy changes, as well as the introduction of new business processes or workflows. Analyses of such changes and of interactions between changes, can reveal how these could modify the attack surface or introduce fragility.

505

[19] See Appendix C.

[20] See Section 2.1.2.

2.1.2 Cyber Resiliency Objectives

Cyber resiliency objectives are more specific statements of what a system must achieve in its operational environment and throughout its life cycle to meet stakeholder needs for mission assurance and resilient security. Cyber resiliency objectives,[21] as described in Table 3, support interpretation, facilitate prioritization and assessment, and enable the development of questions such as:

- What does each cyber resiliency objective mean in the context of the organization and the mission or business process that the system is intended to support?
- Which cyber resiliency objectives are most important to a given stakeholder?
- To what degree can each cyber resiliency objective be achieved?
- How quickly and cost-effectively can each cyber resiliency objective be achieved?
- With what degree of confidence or trust can each cyber resiliency objective be achieved?

TABLE 3: CYBER RESILIENCY OBJECTIVES[22]

OBJECTIVE	DESCRIPTION
PREVENT OR AVOID	Preclude the successful execution of an attack or the realization of adverse conditions.
	Discussion: This objective relates to an organization's preferences for different risk response approaches. Risk avoidance or threat avoidance is one possible risk response approach and is feasible under restricted circumstances. Preventing a threat event from occurring is another possible risk response, similarly feasible under restricted circumstances.
PREPARE	Maintain a set of realistic courses of action that address predicted or anticipated adversity.
	Discussion: This objective is driven by the recognition that adversity will occur. It specifically relates to an organization's contingency planning, continuity of operations plan (COOP), training, exercises, and incident response and recovery plans for critical systems and infrastructures.
CONTINUE	Maximize the duration and viability of essential mission or business functions during adversity.
	Discussion: This objective specifically relates to essential functions. Its assessment is aligned with the definition of performance parameters, analysis of functional dependencies, and identification of critical assets. Note that shared services and common infrastructures, while not identified as essential *per se*, may be necessary to essential functions and thus related to this objective.
CONSTRAIN	Limit damage[23] from adversity.

[21] The term *objective* is defined and used in multiple ways. In this document, uses are qualified (e.g., cyber resiliency objectives, security objectives [FIPS 199], adversary objectives [MITRE18], engineering objectives or purposes [ISO 24765]) for clarity. Cyber resiliency goals and objectives can be viewed as two levels of fundamental objectives, as used in Decision Theory [Clemen13]. Alternately, cyber resiliency goals can be viewed as fundamental objectives and cyber resiliency objectives as enabling objectives [Brtis16]. By contrast, cyber resiliency techniques can be viewed as means objectives [Clemen13].

[22] See Appendix D for specific relationships between objectives and goals.

[23] From the perspective of cyber resiliency, *damage* can be to the organization (e.g., loss of reputation, increased existential risk), missions or business functions (e.g., decrease in the ability to complete the current mission and to accomplish future missions), security (e.g., decrease in the ability to achieve the security objectives of integrity, availability, and confidentiality or decrease in the ability to prevent, detect, and respond to cyber incidents), the system (e.g., decrease in the ability to meet system requirements or unauthorized use of system resources), or specific system elements (e.g., physical destruction; corruption, modification, or fabrication of information).

OBJECTIVE	DESCRIPTION
	Discussion: This objective specifically applies to critical or high-value assets—those cyber assets which contain or process sensitive information, are mission-essential, or provide infrastructure services to mission-essential capabilities.
RECONSTITUTE	Restore as much mission or business functionality as possible after adversity.
	Discussion: This objective relates to essential functions, critical assets, and the services and infrastructures on which they depend. A key aspect of achieving this objective is ensuring that recovery, restoration, or reconstitution efforts result in trustworthy resources. This objective is not predicated on analysis of the source of adversity (e.g., attribution) and can be achieved even without detection of adversity via ongoing efforts to ensure the timely and correct availability of resources.
UNDERSTAND	Maintain useful representations of mission and business dependencies and the status of resources with respect to possible adversity.
	Discussion: This objective supports the achievement of all other objectives, most notably Prepare, Reconstitute, Transform, and Re-Architect. An organization's plans for continuous diagnostics and mitigation (CDM), infrastructure services, and other services support this objective. The detection of anomalies, particularly suspicious or unexpected events or conditions, also supports achieving this objective. However, this objective includes understanding resource dependencies and status independent of detection. This objective also relates to an organization's use of forensics and cyber threat intelligence information sharing.
TRANSFORM	Modify mission or business functions and supporting processes to handle adversity and address environmental changes more effectively.
	Discussion: This objective specifically applies to workflows for essential functions, supporting processes, and incident response and recovery plans for critical assets and essential functions. Tactical modifications are usually procedural or configuration-related; longer-term modifications can involve restructuring operational processes or governance responsibilities while leaving the underlying technical architecture unchanged.
RE-ARCHITECT	Modify architectures to handle adversity and address environmental changes more effectively.
	Discussion: This objective specifically applies to system architectures and mission architectures, which include the technical architecture of the system-of-systems supporting a mission or business function. In addition, this objective applies to architectures for critical infrastructures and services, which frequently support multiple essential functions.

Because stakeholders may find the cyber resiliency objectives difficult to relate to their specific concerns, the objectives can be tailored to reflect the organization's missions and business functions or operational concept for the system-of-interest. Tailoring the cyber resiliency objectives can also help stakeholders determine which objectives apply and the priority to assign to each objective. Cyber resiliency objectives can be hierarchically refined to emphasize the different aspects of an objective or the methods to achieve an objective, thus creating sub-objectives.[24] Cyber resiliency objectives (and, as needed to help stakeholders interpret the objectives for their concerns, sub-objectives) enable stakeholders to assert their different resiliency priorities based on organizational missions or business functions.

[24] Table D-1 in Appendix D provides representative examples of sub-objectives.

2.1.3 Cyber Resiliency Techniques and Approaches

Cyber resiliency goals and objectives provide a vocabulary for describing what properties and capabilities are needed. Cyber resiliency techniques, approaches, and design principles (discussed in Section 2.1.4) provide a vocabulary for discussing how a system can achieve its cyber resiliency goals and objectives. A cyber resiliency technique is a set or class of practices and technologies intended to achieve one or more goals or objectives by providing capabilities. The following 14 techniques are part of the cyber resiliency engineering framework:

1. **Adaptive Response:** Implement agile courses of action to manage risks.
2. **Analytic Monitoring:** Monitor and analyze a wide range of properties and behaviors on an ongoing basis and in a coordinated way.
3. **Contextual Awareness:** Construct and maintain current representations of the posture of missions or business functions considering threat events and courses of action.
4. **Coordinated Protection:** Ensure that protection mechanisms operate in a coordinated and effective manner.
5. **Deception:** Mislead, confuse, hide critical assets from, or expose covertly tainted assets to the adversary.
6. **Diversity:** Use heterogeneity to minimize common mode failures, particularly threat events exploiting common vulnerabilities.
7. **Dynamic Positioning:** Distribute and dynamically relocate functionality or system resources.
8. **Non-Persistence:** Generate and retain resources as needed or for a limited time.
9. **Privilege Restriction:** Restrict privileges based on attributes of users and system elements, as well as on environmental factors.
10. **Realignment:** Structure systems and resource uses to align with mission or business function needs, reduce current and anticipated risks, and accommodate the evolution of technical, operational, and threat environments.
11. **Redundancy:** Provide multiple protected instances of critical resources.
12. **Segmentation:** Define and separate system elements based on criticality and trustworthiness.
13. **Substantiated Integrity:** Ascertain whether critical system elements have been corrupted.
14. **Unpredictability:** Make changes randomly or unpredictably.

The cyber resiliency techniques are described in Appendix D. Each technique is characterized by both the capabilities it provides and the intended consequences of using the technologies or the processes it includes. The cyber resiliency techniques reflect an understanding of the threats as well as the technologies, processes, and concepts related to improving cyber resiliency to address the threats. The cyber resiliency engineering framework assumes that the cyber resiliency techniques will be selectively applied to the architecture or design of organizational mission or business functions and their supporting system resources. Since natural synergies and conflicts exist among the cyber resiliency techniques, engineering trade-offs must be made.

Cyber resiliency techniques are expected to change over time as threats evolve, advances are made based on research, security practices evolve, and new ideas emerge.

Twelve of the 14 cyber resiliency techniques can be applied to either adversarial or non-adversarial threats (including both cyber-related and non-cyber-related threats). The two cyber resiliency techniques specific to adversarial threats are Deception and Unpredictability. The cyber resiliency techniques are also interdependent. For example, the Analytic Monitoring technique supports Contextual Awareness. The Unpredictability technique, however, is different from the other techniques in that it is always applied in conjunction with some other technique (e.g., working with the Dynamic Positioning technique to establish unpredictable times for repositioning potential targets of interest). The definitions of cyber resiliency techniques are intentionally broad to insulate the definitions from changing technologies and threats, thus limiting the need for frequent changes to the set of techniques.

To support detailed engineering analysis, multiple representative approaches to implementing each technique are identified. As illustrated in Figure 1, an *implementation approach* (or, for brevity, an *approach*) is a subset of the technologies and processes included in a technique, defined by how the capabilities are implemented or how the intended outcomes are achieved.

FIGURE 1: CYBER RESILIENCY TECHNIQUES AND IMPLEMENTATION APPROACHES

Table D-4 in Appendix D defines representative approaches and gives representative examples of technologies and practices. The set of approaches for a specific technique is not exhaustive and represents relatively mature technologies and practices. Thus, technologies emerging from research can be characterized in terms of the techniques they apply while not being covered by any of the representative approaches.[25]

2.1.4 Cyber Resiliency Design Principles

A *design principle* refers to a distillation of experience designing, implementing, integrating, and upgrading systems that systems engineers and architects can use to guide and inform design decisions and analysis. A design principle takes the form of a terse statement or a phrase identifying a key concept accompanied by one or more statements that describe how that concept applies to system design (where "system" is construed broadly to include operational processes and procedures and may also include development and maintenance environments). Design principles are defined for many specialty engineering disciplines using the terminology, experience, and research results that are specific to the specialty.

Cyber resiliency design principles, like design principles from other specialty disciplines, can be applied in different ways at multiple stages in the system life cycle, including the operations and maintenance stage. The design principles can also be used in a variety of system development models, including agile and spiral development. The cyber resiliency design principles identified in this publication can serve as a starting point for systems engineers and architects. For any given situation, only a subset of the design principles are selected, and those principles are tailored or "re-expressed" in terms more meaningful to the program, system, or system-of-systems to which they apply.

The cyber resiliency design principles are strongly informed by and can be aligned with design principles from other specialty disciplines, such as the security design principles in [SP 800-160 v1]. Many of the cyber resiliency design principles are based on design principles for security, resilience engineering, or both. Design principles can be characterized as *strategic* (i.e., applied throughout the systems engineering process, guiding the direction of engineering analyses) or *structural* (i.e., directly affecting the architecture and design of the system or system elements) [Ricci14]. Both strategic and structural cyber resiliency design principles can be reflected in security-related systems engineering artifacts. A complete list of strategic and structural cyber resiliency design principles is provided in Appendix D.

2.1.5 Relationship Among Cyber Resiliency Constructs

Cyber resiliency constructs in the form of goals, objectives, techniques, implementation approaches, and design principles enable systems engineers to express cyber resiliency concepts and the relationships among them. In addition, the cyber resiliency constructs also relate to risk management. That relationship leads systems engineers to analyze cyber resiliency solutions in terms of their potential effects on risk and on specific threat events or types of malicious cyber activities. The selection and relative priority of these cyber resiliency constructs is determined by the organization's strategy for managing the risks of depending on systems, which include

[25] Decisions about whether and how to apply less mature technologies and practices are strongly influenced by the organization's risk management strategy. See [SP 800-39].

cyber resources—in particular, by the organization's risk framing.[26] The relative priority of the cyber resiliency goals and objectives and relevance of the cyber resiliency design principles are determined by the risk management strategy of the organization, which takes into consideration the concerns of, constraints on, and equities of all stakeholders (including those who are not part of the organization). Figure 2 illustrates the relationships among the cyber resiliency constructs. These relationships are represented by mapping tables in Appendix D. As Figure 2 illustrates, a cyber-resilient system is the result of the engineering selection, prioritization, and application of cyber resiliency design principles, techniques, and implementation approaches. The risk management strategy for the organization is translated into specific interpretations and prioritizations of cyber resiliency goals and objectives, which guide and inform trade-offs among different forms of risk mitigation.

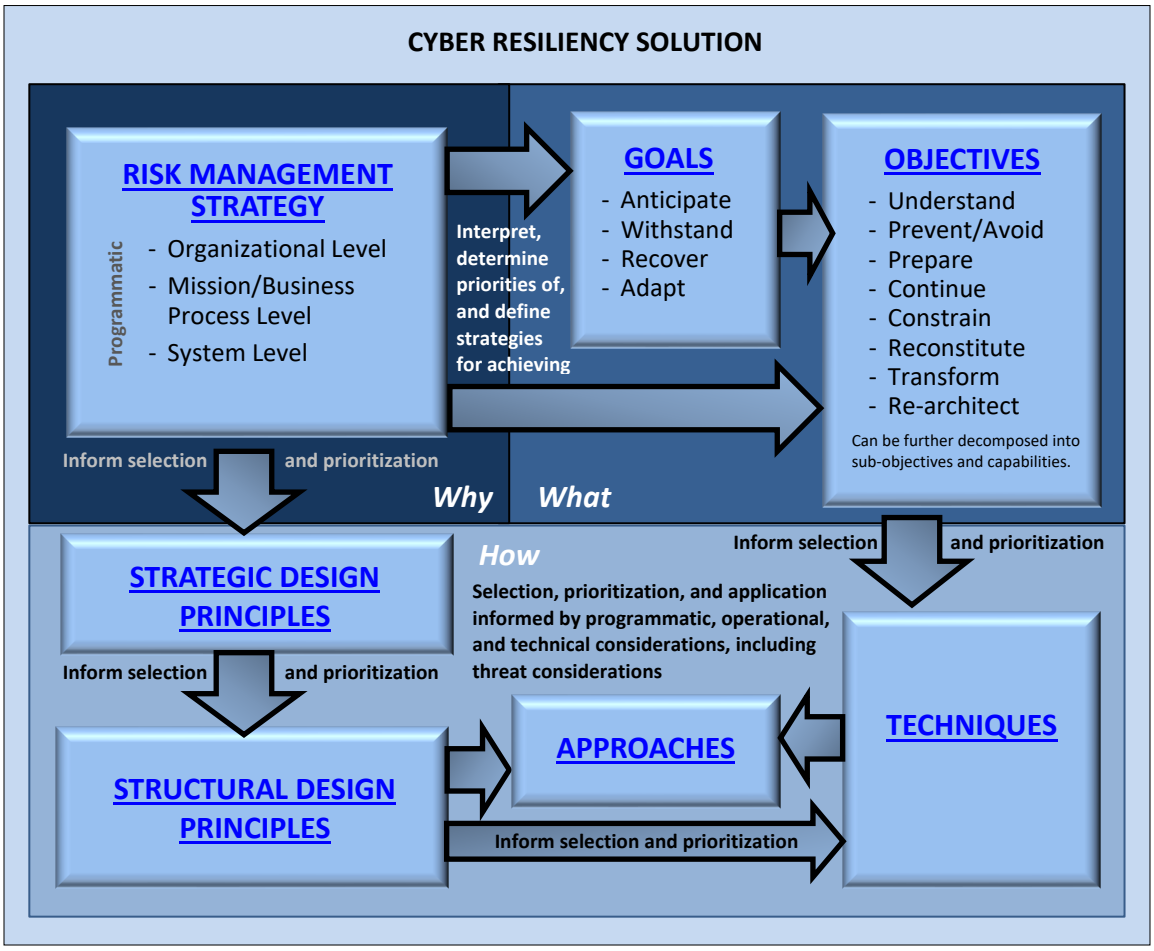

FIGURE 2: RELATIONSHIPS AMONG CYBER RESILIENCY CONSTRUCTS

[26] The first component of risk management addresses how organizations *frame* risk or establish a risk context—that is, describing the environment in which risk-based decisions are made. The purpose of the risk-framing component is to produce a *risk management strategy* that addresses how organizations intend to assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions [SP 800-39]. The risk management strategy addresses how the organization manages the risks of depending on systems that include cyber resources; is part of a comprehensive, enterprise-wide risk management strategy; and reflects stakeholder concerns and priorities.

2.2 CYBER RESILIENCY IN THE SYSTEM LIFE CYCLE

The following section describes general considerations for applying cyber resiliency concepts and framework constructs to system life cycle stages and processes. Considerations include addressing the similarities and differences in security and cyber resiliency terminology and how the application of cyber resiliency goals, objectives, techniques, implementation approaches, and design principles can impact systems at key stages in the life cycle. Figure 3 lists the system life cycle processes and illustrates their application across all stages of the system life cycle. It must be emphasized, however, that cyber resiliency engineering does not assume any specific life cycle or system development process, and cyber resiliency analysis can be performed at any point in and iteratively throughout the life cycle.[27]

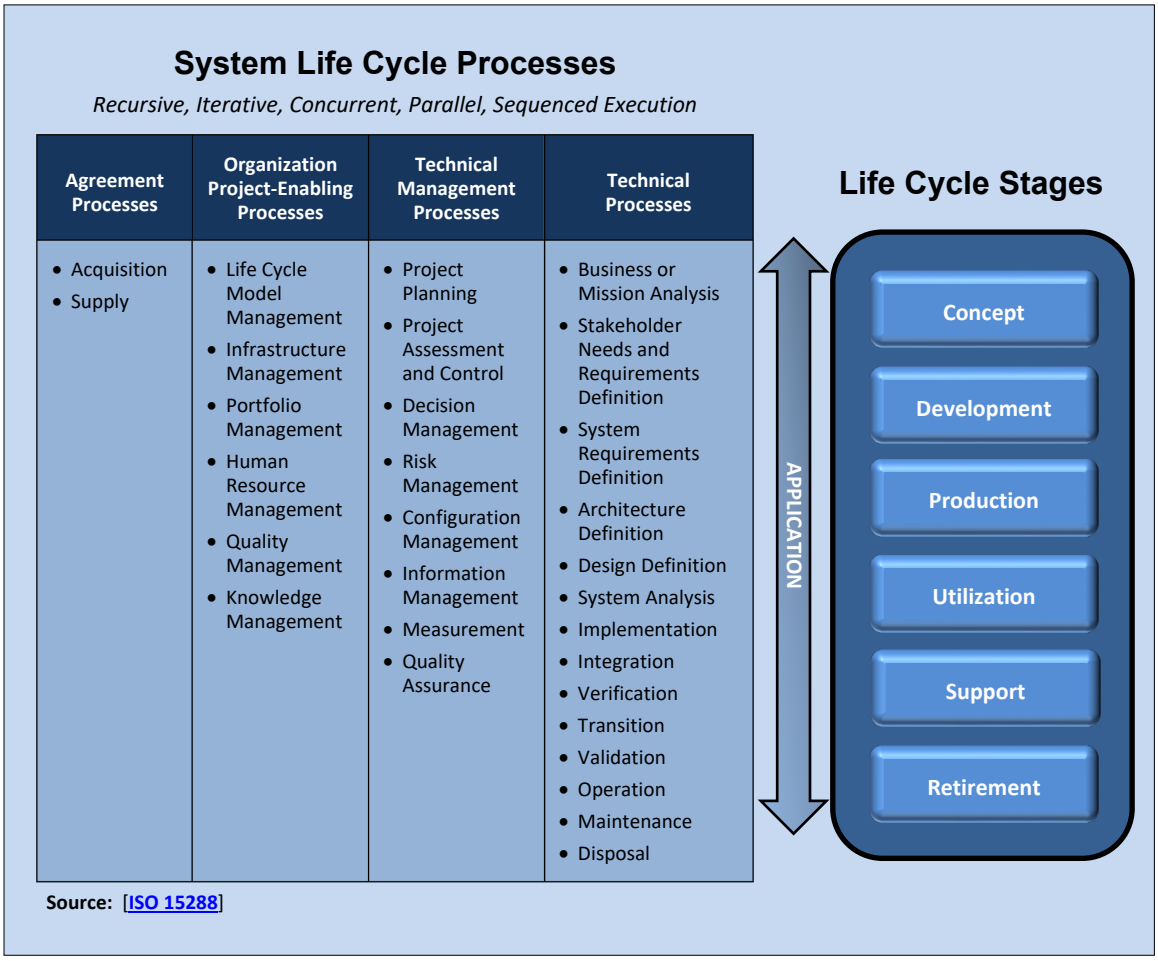

FIGURE 3: SYSTEM LIFE CYCLE PROCESSES AND LIFE CYCLE STAGES

Cyber resiliency constructs are interpreted and cyber resiliency engineering practices are applied in different ways, depending on the system life cycle stages. During the Concept stage, cyber resiliency goals and objectives are tailored in terms of the concept of use for the system-of-interest. Tailoring actions are used to elicit stakeholder priorities for the cyber resiliency goals

[27] See Section 3.2.

and objectives. The organization's risk management strategy is used to help determine which strategic design principles are most relevant. The strategic design principles and corresponding structural design principles are aligned with design principles from other specialty engineering disciplines. Notional or candidate system architectures are analyzed with respect to how well the prioritized cyber resiliency goals and objectives can be achieved and how well the relevant strategic cyber resiliency design principles can be applied. The tailoring of objectives can also be used to identify or define potential metrics or measures of effectiveness for proposed cyber resiliency solutions. Once again, the risk management strategy that constrains risk response or risk treatment (e.g., commitment to specific technologies, requirements for interoperability with or dependence on other systems) is used to help determine which techniques and approaches can or cannot be used in cyber resiliency solutions. In addition, during the *Concept* stage, cyber resiliency concerns for enabling systems for production, integration, validation, and supply chain management are identified, and strategies for addressing those concerns are defined.

During the Development stage, the relevant structural cyber resiliency design principles (i.e., those principles which can be applied to the selected system architecture and which support the strategic cyber resiliency design principles) are identified and prioritized based on how well the design principles enable the prioritized cyber resiliency objectives to be achieved. The cyber resiliency techniques and approaches indicated by the structural design principles are analyzed with respect to whether and where they can be used in the selected system architecture given the constraints identified earlier. Cyber resiliency solutions are defined and analyzed with respect to potential effectiveness and compatibility with other aspects of trustworthiness.

Analysis of potential effectiveness considers the relative effectiveness of the solution against potential threat events or scenarios [SP 800-30] and the measures of effectiveness for cyber resiliency objectives. Analysis of compatibility with other aspects of trustworthiness considers potential synergies or conflicts associated with technologies, design principles, or practices specific to other specialty engineering disciplines, particularly security, reliability, survivability, and safety. In addition, specific measures for assessing whether or not the prerequisite requirements have been satisfied within the solution space are defined. This may include, for example, a determination of the baseline reliability of the technology components needed to deliver cyber-resilient capabilities within a system element.

In addition, during the Development stage, the implementation of cyber resiliency solutions is analyzed and evaluated. The verification strategy for cyber resiliency solutions typically includes adversarial testing or demonstration of mission or business function measures of performance in a stressed environment with adversarial activities. The operational processes and procedures for using technical solutions are defined, refined, and validated with respect to the ability to meet mission and business objectives despite adversity involving systems containing cyber resources. The cyber resiliency perspective calls for testing and other forms of validation or verification that include adversarial threats among (and in combination with) other stresses on the system. During this life cycle stage, resources (e.g., diverse implementations of critical system elements, alternative processing facilities) required to implement specific courses of action are also developed.

During the Production stage, the verification strategy is applied to instances or versions of the system-of-interest and associated spare parts or components. The verification strategy for the cyber resiliency requirements as applied to such instances and system elements includes

adversarial testing or demonstration in a stressed environment. In addition, during the Production stage, cyber resiliency concerns for enabling systems for production, integration, validation, and supply chain management continue to be identified and addressed.

During the Utilization stage, the effectiveness of cyber resiliency solutions in the operational environment is monitored. Effectiveness may decrease due to changes in the operational environment (e.g., new mission or business processes, increased user population, deployment in new locations, addition or removal of other systems or system elements with which the system-of-interest interacts), the threat environment (e.g., new threat actors, new vulnerabilities in commonly used technologies), or the technical environment (e.g., the introduction of new technologies into other systems with which the system-of-interest interacts). Cyber resiliency solutions may need to be adapted to address such changes (e.g., defining new courses of action, changing mission or business processes and procedures, reconfiguring system elements). New stakeholders may arise from changes in the operational environment, and their concerns may change the relative priorities of cyber resiliency objectives. Changes in the threat or technical environment may make some techniques or approaches less feasible, while changes in the technical or operational environment may make others more viable.

During the Support stage, maintenance and upgrade of the system or system elements can include integration of new cyber resiliency solutions into the system-of-interest. This stage also provides opportunities to revisit the prioritization and tailoring of cyber resiliency objectives. Upgrades to or modifications of system capabilities can include significant architectural changes that address accumulated changes to the operational, threat, and technical environments. System modifications and upgrades can also introduce additional vulnerabilities, particularly with architectural changes.

During the Retirement stage, system elements or the entire system-of-interest are removed from operations. The retirement process can affect other systems with which the system-of-interest interacts and can decrease the cyber resiliency of those systems and of the supported mission or business processes. Retirement strategies can include phased removal of system elements, turnkey removal of all system elements, phased replacement of system elements, and turnkey replacement of the entire system-of-interest. Cyber resiliency objectives and priorities are identified for the systems, missions, and business functions in the operational environment to inform analysis of the potential or expected effects of different retirement strategies on the ability to achieve those objectives. Like the support stage, the retirement stage can introduce significant vulnerabilities, particularly during disposal and unintended residue remaining from decommissioned assets.

Table 4 illustrates changes in emphasis for the different cyber resiliency constructs, particularly with respect to cyber resiliency objectives (**bolded**).

TABLE 4: CYBER RESILIENCY IN LIFE CYCLE STAGES

LIFE CYCLE STAGES	ROLE OF CYBER RESILIENCY CONSTRUCTS
CONCEPT	- Prioritize and tailor objectives. - Prioritize design principles and align with other disciplines. - Limit the set of techniques and approaches to use in solutions.

LIFE CYCLE STAGES	ROLE OF CYBER RESILIENCY CONSTRUCTS
DEVELOPMENT	- Apply design principles to analyze and shape architecture and design. - Use techniques and approaches to define alternative solutions. - Develop capabilities to achieve the **Prevent/Avoid**, **Continue**, **Constrain**, **Reconstitute**, and **Understand** objectives.
PRODUCTION	- Implement and evaluate the effectiveness of cyber resiliency solutions. - Provide resources (or ensure that resources will be provided) to achieve the **Prepare** objective.
UTILIZATION	- Monitor the effectiveness of cyber resiliency solutions using capabilities to achieve **Understand** and **Prepare** objectives. - Reprioritize and tailor objectives as needed, and adapt mission, business, and/or security processes to address environmental changes (**Transform** objective).
SUPPORT	- Revisit the prioritization and tailoring of objectives; use the results of monitoring to identify new or modified requirements. - Revisit constraints on techniques and approaches. - Modify or upgrade capabilities consistent with changes as noted (**Re-Architect** objective).
RETIREMENT	- Prioritize and tailor objectives for the environment of operation. - Ensure that disposal processes enable those objectives to be achieved, modifying or upgrading capabilities of other systems as necessary (**Re-Architect** objective).

2.3 RISK MANAGEMENT AND CYBER RESILIENCY

Organizations manage the missions, business functions, and operational risks related to a dependence on systems that include cyber resources as part of a larger portfolio of risks,[28] including financial and reputational risks; programmatic or project-related risks associated with developing a system (e.g., cost, schedule, performance); security risks associated with the organization's mission or business activities, information the organization processes or handles, or requirements arising from legislation, regulations, policies, or standards; and cybersecurity risks. A proposed cyber resiliency solution, while intended primarily to reduce mission, business, or operational risk, can also reduce other types of risk (e.g., security risk, reputational risk, supply chain risk, performance risk). However, like any solution to a risk management problem, it can also increase other types of risk (e.g., financial, cost, or schedule risk). As part of a multidisciplinary systems engineering effort, systems security engineers and risk management professionals are responsible for articulating the potential risk impacts of alternative solutions, determining whether those impacts fall within the organizational risk tolerance, deciding whether the adoption of a proposed solution is consistent with the organization's risk management strategy, and informing the organization's risk executive (function) of risk trade-offs.[29]

[28] These risks are typically addressed by organizations as part of an Enterprise Risk Management (ERM) program. See [IR 8286].

[29] See Section 3.2.1 and Section C.4.

771 At the organizational level, a cyber resiliency perspective on risk management can lead to
772 analysis of and management of risks associated with programs and initiatives at multiple levels,
773 which involve investment in, transition to, use of, or transition away from different cyber
774 technologies. The environment in which a system-of-interest is engineered is rarely static.
775 Related programs, initiatives, or other efforts can include programs at federal agencies to
776 transition to a zero trust architecture, initiatives to reduce software supply chain risks driven by
777 [EO 14028], and initiatives to transition to IPv6 and away from IPv4. Such organization-level
778 programs and initiatives can affect the execution of efforts at lower levels (e.g., an acquisition
779 program for a specific system or service, an initiative to redefine a mission or business process
780 to better accommodate telework).

781 Motivated by the cyber resiliency Adapt goal, an organization's risk management strategy can
782 call for the analysis of questions such as:

783 • How does each step in a transition plan or an investment plan change the attack surface?

784 • Are new attack vectors enabled by a given step? How will they be mitigated? Will they be
785 removed in a later step?

786 • Does this step increase fragility, complexity, or instability, and if so, how will those risks be
787 managed?

788 • On what other programs or initiatives does this step depend, and how will the risks that
789 those efforts will not achieve the expected objectives be managed?

790 • What new or modified operational procedures and processes are assumed, and how will
791 they be resourced and staffed?

792 • What policy or governance changes are assumed? How will they be achieved? What risks
793 would result if they are not achieved?

794 • How will the cyber resiliency objectives (as interpreted and prioritized by the organization)
795 continue to be achieved in the face of changes resulting from different programs and
796 initiatives?

797

798

GENERALIZED CYBER RESILIENCY CONSTRUCTS

The definitions of the cyber resiliency goals, objectives, and techniques are generally defined so that they can be applied to all types of threats (not solely cyber threats) and all types of systems (not solely systems that include or are enabled by cyber resources). However, the motivation for these definitions and for the selection of objectives and techniques for inclusion in the cyber resiliency engineering framework is the recognition of dependence on systems involving cyber resources in a threat environment that includes the APT.

799

CHAPTER THREE

CYBER RESILIENCY IN PRACTICE

APPLYING CYBER RESILIENCY CONCEPTS, CONSTRUCTS, PRACTICES

This chapter identifies considerations for determining which cyber resiliency constructs are most relevant to a system-of-interest and describes a tailorable process for applying cyber resiliency concepts, constructs, and practices to a system. It also includes guidance on the cyber resiliency analysis carried out during the system life cycle to determine whether the cyber resiliency properties and behaviors of a system-of-interest, regardless of its life cycle stage, are sufficient for the organization using that system to meet its mission assurance, business continuity, or other security requirements in a threat environment and contested cyberspace that includes the APT.

3.1 SELECTING AND PRIORITIZING CYBER RESILIENCY CONSTRUCTS

The variety of concerns, technologies, and practices related to cyber resiliency results in an extensive framework for cyber resiliency engineering. For example, the engineering framework identifies 14 cyber resiliency techniques and 50 cyber resiliency implementation approaches. The engineering framework is also complex, with relationships among the constructs of goals, objectives, design principles, techniques, and approaches as discussed in Appendix D. Cyber resiliency design principles, techniques, and approaches build on, complement, or function in synergy with mechanisms intended to ensure other quality properties (e.g., security, safety, and system resilience).

The variety of circumstances and types of systems for which cyber resiliency can be applied means that no single cyber resiliency technique, approach, or set of approaches is universally optimal or applicable. Systems security engineering seeks to manage risk rather than provide a universal solution. The choice of a risk-appropriate set of cyber resiliency techniques and approaches depends on various trade space considerations and risk factors that are assessed during the systems engineering processes. Employing all cyber resiliency techniques and approaches is not needed to achieve the cyber resiliency objectives prioritized by stakeholders. In fact, it is not possible to employ all techniques and approaches simultaneously. The following subsections describe factors to consider when selecting a set of cyber resiliency techniques and implementation approaches that best fits the system-of-interest.

3.1.1 Achievement of Goals and Objectives

Cyber resiliency techniques and associated implementation approaches are employed to achieve mission or business objectives. The relative priorities of cyber resiliency goals and objectives are determined by the mission or business objectives. The selection of specific cyber resiliency techniques and approaches is therefore driven in part by the relative priorities of the objectives they support.[30]

[30] See Appendix D, Table D-13.

3.1.2 Cyber Risk Management Strategy

An organization's cyber risk management strategy (i.e., its strategy for managing risks stemming from dependencies on systems which include cyber resources) is part of its risk management strategy and includes its risk framing for cyber risks.[31] The organization's risk frame identifies which risks or risk factors (i.e., potential impacts or consequences) are unacceptable. For cyber resiliency, the risk frame assumes an advanced adversary with a persistent presence in organizational systems. The risk response portion of the risk management strategy can include priorities or preferences for the types of effects on adversary activities[32] to seek in cyber resiliency solutions.

An organization's risk management strategy is constrained by such factors as legal, regulatory, and contractual requirements as reflected in organizational policies and procedures; financial resources; legacy investments; and organizational culture. These constraints can be reflected in the selection and tailoring of cyber resiliency techniques, approaches, and design principles. For example, organizational policies and culture can strongly influence whether and how the cyber resiliency technique of Deception is used. The risk management strategy can define an order of precedence for responding to identified risks analogous to the safety order of precedence, such as "harden, sensor, isolate, obfuscate." Together with the strategic design principles selected and specifically tailored to a given program, mission, business function, or system, the order of precedence can guide the selection and application of structural design principles at different locations in an architecture.[33]

3.1.3 System Type

The set of cyber resiliency techniques and approaches which are most relevant to and useful in a system depends on the type of system. The following present some general examples of system types and examples of techniques and approaches that might be appropriate for those types of systems. Additional (more specific) examples are provided at the SP 800-160, Volume 2 website. In addition to the techniques and approaches listed in the examples below, there may be other techniques and approaches that could be useful for a particular type of system. The specific aspects of the system in question will impact the selection as well.

- **Enterprise IT Systems, Shared Services, and Common Infrastructures**

  Enterprise IT (EIT) systems are typically general-purpose computing systems—very often with significant processing, storage, and bandwidth—capable of delivering information resources which can meet the business or other mission needs of an enterprise or a large stakeholder community. As such, all of the cyber resiliency techniques and associated approaches may potentially be viable, although their selection would depend on the other considerations noted in this section.

[31] Risk management consists of four major components: risk framing, risk assessment, risk response, and risk monitoring [SP 800-39]. Security risks are considered throughout an organization's enterprise risk management (ERM) process. This includes identifying the risk context; identifying, analyzing, and prioritizing risks; planning and executing risk response strategies; and monitoring, evaluating, and adjusting risk [IR 8286]. Risk response is also referred to as risk treatment [SP 800-160 v1] [ISO 73]. Organizational risk tolerance is determined as part of the risk framing component and defined in the risk management strategy [SP 800-39].

[32] See Appendix F.

[33] See Appendix D.

- **Large-Scale Processing Environments**

  Large scale processing environments (LSPEs) handle large numbers of events (e.g., process transactions) with high confidence in service delivery. The scale of such systems makes them highly sensitive to disruptions to or degradation of service. Therefore, the selective use of the Offloading and Restriction implementations approaches can make the scale of such systems more manageable. This, in turn, will support the application of Analytic Monitoring and the Mission Dependency and Status Visualization approach to Contextual Awareness in a manner that does not significantly affect performance. LPSEs often implement Dynamic Positioning functionality that can be repurposed to help improve cyber resiliency via the Functional Relocation of Cyber Resources, Fragmentation, and Distributed Functionality approaches.

- **System-of-Systems**

  Many cyber resiliency techniques are likely to be applicable to a system-of-systems, but some techniques and approaches can offer greater benefits than others. For example, Contextual Awareness implemented via Mission Dependency and Status Visualization can be applied to predict the potential mission impacts of cyber effects of adversary activities on constituent systems or system elements. The Calibrated Defense-in-Depth and Consistency Analysis approaches to the technique of Coordinated Protection can help ensure that the disparate protections of the constituent systems operate consistently and in a coordinated manner to prevent or delay the advance of an adversary across those systems. For a system-of-systems involving constituent systems that were not designed to work together and that were developed with different missions, functions, and risk frames, Realignment could also be beneficial. In particular, the Offloading and Restriction approaches could be used to ensure that the core system elements are appropriately aligned to the overall system-of-system mission.

- **Critical Infrastructure Systems**

  Critical infrastructure systems are often specialized, high-confidence, dedicated, purpose-built systems that have highly deterministic properties. Therefore, the availability and integrity of the functionality of the systems are very important as the corruption or lack of availability of some of the key system elements could result in significant harm. For these reasons, techniques adapted from system resilience, such as Redundancy (particularly the Protected Backup and Restore and Surplus Capacity approaches) coupled with aspects of Diversity (e.g., Architectural Diversity, Supply Chain Diversity), could prevent attacks from having mission or business consequences and also maximize the chance of continuation of the critical or essential mission or business operations. Segmentation can isolate highly critical system elements to protect them from an adversary's activities. Approaches such as Trust-Based Privilege Management and Attribute-Based Usage Restriction could constrain the potential damage that an adversary could inflict on a system.

- **Cyber-Physical Systems**

  As with critical infrastructure systems, cyber-physical systems (CPS) often have significant limitations regarding storage capacity, processing capabilities, and bandwidth. In addition, many of these systems have a high degree of autonomy with limited human interaction. Some cyber-physical systems operate with no active network connection, although they may connect to a network under specific circumstances (e.g., scheduled maintenance). Non-

Persistent Services support the periodic refreshing of software and firmware from a trusted source (e.g., an offline redundant component), in effect flushing out any malware. However, that approach applies only if the organization can allow for the periodic downtime that the refresh would entail. Similarly, the Integrity Checks approach to Substantiated Integrity implemented via cryptographic checksums on critical software could help enable embedded systems to detect corrupted software components.

- **Internet of Things**

  An Internet of Things (IoT) system consists of system elements with network connectivity, which communicate with an Internet-accessible software application. That software application, which is part of the IoT system, orchestrates the behavior of or aggregates the data provided by constituent system elements. As in a cyber-physical system, the system elements have limitations in the areas of power consumption, processing, storage capacity, and bandwidth, which in turn may limit the potential for such processing-intensive cyber resiliency approaches as Obfuscation or Adaptive Management at the device level. Because many "things" (e.g., light bulbs, door locks) are small and relatively simple, they often lack the capacity for basic protection. However, the Integrity Checks approach to Substantiated Integrity could still be viable, applied in conjunction with reliability mechanisms. An IoT system assumes Internet connectivity, although the set of "things" are usually capable of functioning independently if not connected. Because many IoT systems do not assume technical expertise on the part of users, cyber resiliency techniques and approaches that involve human interaction (e.g., Disinformation, Misdirection) may not be appropriate. In addition, the design of IoT systems accommodates flexibility and repurposing of the capabilities of constituent "things." Thus, an application that orchestrated the behavior of one set of "things" may be upgraded to orchestrate additional sets, the members of which were not designed with that application in mind. Such changes to the IoT systems to which that application or the additional sets originally belong can benefit from the application of Realignment. At the level of an IoT system (rather than at the level of individual system elements), Segmentation and Consistency Analysis can be applied.

3.1.4 Cyber Resiliency Conflicts and Synergies

Cyber resiliency techniques can interact in several ways. One technique can depend on another so that the first cannot be implemented without the second; for example, Adaptive Response depends on Analytic Monitoring or Contextual Awareness since a response requires a stimulus. One technique can support another, making the second more effective; for example, Diversity and Redundancy are mutually supportive. One technique can use another so that more design options are available than if the techniques were applied independently; for example, Analytic Monitoring can use Diversity in a design, which includes a diverse set of monitoring tools.

However, one technique can also conflict with or complicate the use of another. For example, Diversity and Segmentation can each make Analytic Monitoring and Contextual Awareness more difficult; a design that incorporates Diversity requires monitoring tools that can handle the diverse set of system elements, while implementation of Segmentation can limit the visibility of such tools. In selecting techniques in accordance with the risk management strategy and design principles, synergies and conflicts between various techniques are taken into consideration. The text below offers three illustrative examples of the interplay, focusing on the techniques that increase an adversary's work factor.

As a first example, Dynamic Positioning and Non-Persistence enable operational agility by making it more difficult for an adversary to target critical resources. These techniques support the Continue, Constrain, and Reconstitute objectives and are part of applying the Support agility and architect for adaptability strategic design principle and the Change or disrupt the attack surface structural design principle. At the same time, these techniques (and the associated implementation approaches) also make it more difficult for an organization to maintain situational awareness of its security posture. That is, Dynamic Positioning and Non-Persistence complicate the use of Contextual Awareness and aspects of Analytic Monitoring, and thus can conflict with the Maintain situational awareness structural design principle.

As a second example, Redundancy and Diversity together are effective at resisting adversary attacks. These techniques enhance the system's ability to achieve the Continue and Reconstitute objectives and apply the Plan and manage diversity and Maintain redundancy structural design principles. However, the implementation of both Redundancy and Diversity will increase the system's attack surface.

As a final example, Deception can lead the adversary to waste effort and reveal tactics, techniques, and procedures (TTP), but it can also complicate the use of aspects of Analytic Monitoring and Contextual Awareness. In general, while Redundancy, Diversity, Deception, Dynamic Positioning, and Unpredictability will likely greatly increase the adversary work factor, they come at a cost to some other cyber resiliency objectives, techniques, and design principles.

No technique or set of techniques is optimal with respect to all decision factors. There are always ramifications for employing any given technique. The determination of the appropriate selection of techniques is a trade decision that systems engineers make. A more complete identification of potential interactions (e.g., synergies and conflicts) between cyber resiliency techniques is presented in Table D-3.

3.1.5 Other Disciplines and Existing Investments

Many of the techniques and implementation approaches supporting cyber resiliency are well-established. Some technologies or processes are drawn from other disciplines (e.g., Continuity of Operations [COOP], cybersecurity) but are used or executed in a different manner to support cyber resiliency. These include Adaptive Response, Analytic Monitoring, Coordinated Protection, Privilege Restriction, Redundancy, and Segmentation. Others are drawn from disciplines that deal with non-adversarial threats (e.g., safety, reliability, survivability). These include Contextual Awareness, Diversity, Non-Persistence, Realignment, and Substantiated Integrity. Still others are cyber adaptations of non-cyber concepts drawn from disciplines that deal with adversarial threats (e.g., medicine, military, sports). These include Deception, Dynamic Positioning, and Unpredictability. Legacy investments made by an organization in these other disciplines can influence which cyber resiliency techniques and approaches are most appropriate to pursue.

3.1.5.1 Investments from Cybersecurity, COOP, and Resilience Engineering

Redundancy-supporting approaches—such as backup, surplus capacity, and replication—are well-established in COOP programs. From a cyber resiliency perspective, however, these approaches are not sufficient to protect against the APT. A threat actor might choose to target backup servers as optimum locations to implant malware if those servers are not sufficiently protected. In addition, remote backup servers that employ the same architecture as the primary

server are vulnerable to malware that has compromised the primary server. However, if an organization has already invested in backup services (in support of COOP or cybersecurity), those services can be enhanced by requiring an adversary to navigate multiple distinct defenses, authentication challenges (Calibrated Defense-in-Depth approach to Coordinated Protection), or some form of Synthetic Diversity to compensate for known attack vectors.

Contextual Awareness and Analytic Monitoring capabilities are often provided by performance management and cybersecurity functions, including cyber situational awareness, anomaly detection, and performance monitoring. However, the off-the-shelf implementations of these functions are generally insufficient to detect threats from advanced adversaries. Enhancing existing investments in both detection and monitoring by integrating data from sensor and monitor readings from disparate sources is a way to take these existing investments and make them an effective cyber resiliency tool. Another way to make existing technology more cyber-resilient is to complement the existing monitoring services with information from threat intelligence sources, enabling these tools to be better-tuned to look for known observables (e.g., indicators of adversary TTPs).

Some approaches to Segmentation and Coordinated Protection appear in information security or cybersecurity. Predefined Segmentation, as reflected in boundary demilitarized zones (DMZs), is a well-established construct in cybersecurity. One important distinction of cyber resiliency is that the segmentation is applied throughout the system, not just at the system boundary. In addition, the Dynamic Segmentation and Isolation approach allows for changing the placement and/or activation of the protected segments. For Coordinated Protection, the defense-in-depth approach is often used for security or system resilience. Ensuring that those protections work in a coordinated fashion is one of the distinguishing aspects of cyber resiliency.

3.1.5.2 Investments from Non-Adversarial Disciplines

Some cyber resiliency techniques and approaches come from disciplines such as safety or performance management. Diversity and certain implementations of Substantiated Integrity, such as Byzantine quorum systems[34] or checksums on critical software, can be traced back to the safety discipline.[35] Therefore, systems that have been designed with safety in mind may already have implemented some of these capabilities. However, the safety capabilities were designed with the assumption that they were countering non-adversarial threat events. To make these capabilities useful against the APT, certain changes are needed. From a safety perspective, it may be sufficient to only employ polynomial hashes on critical software to ensure that the software has not been corrupted over time. However, such hashes are not sufficient when dealing with the APT, which is able to corrupt the software and data and then recalculate the checksum. Instead, what is needed in those instances are cryptographic-based polynomial checksums.

Other capabilities such as Non-Persistence and Adaptive Response are very common in cloud and virtualization architectures. Again, these capabilities were not designed or employed to

[34] The National Aeronautics and Space Administration (NASA) Space Shuttle Program applied this concept in multiple computers, which would vote on certain maneuvers.

[35] This is an example of *operational redundancy* where specific failure modes are managed as part of the nominal operation of the system. Redundant Array of Independent Disks (RAID) storage systems and "hyper-converged" computing architectures (i.e., those relying on erasure code for distributed data stores) also fall into this category.

specifically counter the APT but to facilitate rapid deployment of implementations. From a system design and implementation perspective, it is most likely easier to employ existing virtualization technology and change the criteria of when and why to refresh critical services (e.g., periodically refresh the software and firmware with the goal of flushing out malware) than it is to deploy Non-Persistence in a system that cannot implement the capability.

3.1.5.3 Investments from Adversarial Disciplines

Several of the cyber resiliency techniques and approaches are cyber adaptions of non-cyber methods used in adversary-oriented disciplines (e.g., medicine, military, sports). These include the Deception, Unpredictability, and Dynamic Positioning techniques and the Dynamic Threat Awareness and Evolvability approaches. None of those techniques or approaches are employed in non-adversarial disciplines. These is no reason in resilience engineering to attempt to "mislead" a hurricane, nor is there any benefit in safety engineering to include an element of unpredictability. The value of these constructs in non-cyber environments is well established. Because these adversarial-derived techniques and approaches are not typically found in disciplines such as safety, resilience engineering, or COOP, it is much more challenging to provide them by enhancing existing constructs. Therefore, they may be more challenging to integrate into an existing system.

3.1.6 Architectural Locations

The selection of cyber resiliency techniques or approaches depends, in part, on where (i.e., at what layers, in which components or system elements, at which interfaces between layers or between system elements) in the system architecture cyber resiliency solutions can be applied. The set of layers, like the set of system components or system elements, in an architecture depends on the type of system. For example, an embedded system offers a different set of possible locations than an enterprise architecture that includes applications running in a cloud. The set of possible layers can include, for example, an operational (people-and-processes) layer, a support layer, and a layer to represent the physical environment.

Different cyber resiliency techniques or approaches lend themselves to implementation at different architectural layers.[36] Some approaches can be implemented at multiple layers, in different ways, and with varying degrees of maturity. Other approaches are highly specific to a layer; for example, Asset Mobility is implemented in the operations layer or in the physical environment. For some layers, many approaches may be applicable; for others, relatively few approaches may be available. For example, relatively few approaches can be implemented at the hardware layer. These include Dynamic Reconfiguration, Architectural Diversity, Design Diversity, Replication, Predefined Segmentation, and Integrity Checks.

Similarly, some cyber resiliency approaches lend themselves to specific types of components or system elements. For example, Fragmentation applies to information stores. Some approaches assume that a system element or set of system elements has been included in the architecture specifically to support cyber defense. These include Dynamic Threat Awareness, Forensic and Behavioral Analysis, and Misdirection. Other cyber resiliency approaches assume that a system element has been included in the architecture, explicitly or virtually, to support the mission,

[36] See Appendix D, Table D-4.

security, or business operations. These include Sensor Fusion and Analysis, Consistency Analysis, Orchestration, and all of the approaches to Privilege Restriction.

Finally, some techniques or approaches lend themselves to implementation at interfaces between layers or between system elements. These include Segmentation, Monitoring and Damage Assessment, and Behavior Validation.

3.1.7 Effects on Adversaries, Threats, and Risks

The selection of cyber resiliency techniques and approaches can be motivated by potential effects on adversary activities or on risk. Two resiliency techniques or approaches listed as both potentially having the same effect may differ in how strongly that effect applies to a given threat event, scope (i.e., the set of threat events for which the effect is or can be produced), and affected risk factors. For example, all approaches to Non-Persistence can degrade an adversary's ability to maintain a covert presence via the malicious browser extension TTP; closing the browser session when it is no longer needed, a use of Non-Persistent Services, degrades the adversary's activity more than do the other Non-Persistence approaches. Some techniques or approaches will affect more risk factors (e.g., reduce the likelihood of impact or reduce the level of impact) than others. The security mechanisms or processes used to implement a particular cyber resiliency approach will also vary with respect to their scope and strength. For example, a Misdirection approach to the Deception technique, implemented via a deception net, and the Sensor Fusion and Analysis approach to Analytic Monitoring, implemented via a holistic suite of intrusion detection systems, will both achieve the detect effect. However, the effectiveness and scope of the two vary widely. For this reason, engineering trade-offs among techniques, approaches, and implementations should consider the actual effects to be expected in the context of the system's architecture, design, and operational environment.

In general, systems security engineering decisions seek to provide as complete a set of effects as possible and to maximize those effects with the recognition that this optimization problem will not have a single solution. The rationale for selecting cyber resiliency techniques or approaches that have complete coverage of the potential effects relates to the long-term nature of the threat campaigns. Potentially, engagements with the APT may go on for months, if not years, possibly starting while a system is in development or even earlier in the life cycle. Given the nature of the threat, its attacks will likely evolve over time in response to a defender's actions. Having a selection of techniques and approaches—where each technique and approach supports (to different degrees and in different ways) multiple effects on the adversary, and the union of the techniques and approaches allows for all potential effects on an adversary—provides the systems engineers with the flexibility to evolve and tailor the effects to the adversary's changing actions. This is analogous to team sports where a team will change its game plan in response to player injuries and the changing game plan of the other team. A team with players who can play multiple positions gives it the flexibility to respond to changes by the opposition and to potentially replace injured players.

Different cyber resiliency techniques and approaches can have different effects on threat events and risk. No single technique or approach can create all possible effects on a threat event, and no technique or approach or set of techniques or approaches can eliminate risk. However, by

considering the desired effects, systems engineers can select a set of techniques that will collectively achieve those effects.[37]

3.1.8 Maturity and Potential Adoption

Approaches to applying cyber resiliency techniques vary in maturity and adoption. The decision to use less mature technologies depends on the organization's risk management strategy and its strategy for managing technical risks. Many highly mature and widely adopted technologies and processes that were developed to meet the general needs of performance, dependability, or security can be used or repurposed to address cyber resiliency concerns. These pose little, if any, technical risk. Changes in operational processes, procedures, and configuration changes may be needed to make these technologies and processes effective against the APT and thus part of cyber resiliency solutions.

A growing number of technologies are specifically oriented toward cyber resiliency, including moving target defenses and deception toolkits. These technologies are currently focused on enterprise IT environments. As these technologies become more widely adopted, the decision to include the technologies is influenced more by policy than by technical risk considerations. This is particularly the case for applications of the Deception and Unpredictability cyber resiliency techniques.

Cyber resiliency is an active research area. Technologies are being explored to improve the cyber resiliency of cyber-physical systems, high-confidence dedicated-purpose systems, and large-scale processing environments. The integration of solutions involving new technologies to reduce risks due to the APT should be balanced against risks associated with perturbing such systems.

3.2 ANALYTIC PRACTICES AND PROCESSES

In the context of systems security engineering, cyber resiliency analysis is intended to determine whether the cyber resiliency properties and behaviors of a system-of-interest, regardless of its system life cycle stage, are sufficient for the organization using that system to meet its mission assurance, business continuity, or other security requirements in a threat environment that includes the APT. Cyber resiliency analysis is performed with the expectation that such analysis will support systems engineering and risk management decisions about the system-of-interest. Depending on the life cycle stage, programmatic considerations, and other factors discussed above, a cyber resiliency analysis could recommend architectural changes, the integration of new products or technologies into the system, changes in how existing products or technologies are used, or changes in operating procedures or environmental protections consistent with and designed to implement the organization's risk management strategy.

The following subsections describe a general, tailorable process for cyber resiliency analysis consisting of steps and tasks, as summarized in Table 5. A variety of motivations for a cyber resiliency analysis are possible, including ensuring that cyber risks due to the APT are fully considered as part of the RMF process or other risk management process, supporting systems security engineering tasks, and recalibrating assessments of risk and risk responses based on information about new threats (e.g., information about a cyber incident or an APT actor), newly

[37] See Appendix F.

discovered vulnerabilities (e.g., discovery of a common design flaw), and problematic dependencies (e.g., discovery of a supply chain issue). Although described in terms of a broad analytic scope, the process can be tailored to have a narrow scope, such as analyzing the potential cyber resiliency improvement that could be achieved by integrating a specific technology or identifying ways to ensure adequate cyber resiliency against a specific threat scenario.

The analytic processes and practices related to cyber resiliency are intended to be integrated with those for other specialty engineering disciplines, including security, systems engineering, resilience engineering, safety, cybersecurity, and mission assurance.[38] In addition, analytic processes and practices related to cyber resiliency can leverage system representations offered by model-based systems engineering (MBSE) and analytic methods (including those involving artificial intelligence [AI] and machine learning [ML]) integrated into MBSE.

A variety of artifacts can provide information used in a cyber resiliency analysis depending on its scope, the life cycle stage of the system or systems within the scope of the analysis, the step in the RMF of the in-scope system or systems, the extent to which the organization relying on the system or systems has done contingency planning, and (for systems in the Utilization life cycle stage) reports on security posture and incident response. These artifacts can include engineering project plans, system security plans, supply chain risk management plans [SP 800-161], reports on security posture [SP 800-37], penetration test results, contingency plans [SP 800-34], risk analyses [SP 800-30], after-action reports from exercises, incident reports, and recovery plans.

Cyber resiliency analysis complements both system life cycle and RMF tasks. The life cycle and RMF tasks produce information that can be used in cyber resiliency analysis, and cyber resiliency analysis enables cyber risks to be considered more fully in life cycle and RMF tasks.

TABLE 5: TAILORABLE PROCESS FOR CYBER RESILIENCY ANALYSIS

ANALYSIS STEP	MOTIVATING QUESTION	TASKS
Understand the context	How do stakeholder concerns and priorities translate into cyber resiliency constructs and priorities?	• Identify the programmatic context. • Identify the architectural context. • Identify the operational context. • Identify the threat context. • Interpret and prioritize cyber resiliency constructs.
Establish the initial cyber resiliency baseline	How well is the system doing (i.e., how well does it meet stakeholder needs and address stakeholder concerns) with respect to the aspects of cyber resiliency that matter to stakeholders?	• Identify existing capabilities. • Identify gaps and issues. • Define evaluation criteria and make an initial assessment.
Analyze the system	How do cyber risks affect mission, business, or operational risks?	• Identify critical resources, sources of fragility, and attack surfaces. • Represent the adversary perspective. • Identify and prioritize opportunities for improvement.

[38] See Section D.3.

ANALYSIS STEP	MOTIVATING QUESTION	TASKS
Define and analyze specific alternatives	How can mission or operational resilience be improved by improving cyber resiliency?	• Define potential technical and procedural solutions. • Define potential solutions for supporting systems and processes. • Analyze potential solutions with respect to criteria.
Develop recommendations	What is the recommended plan of action?	• Identify and analyze alternatives. • Assess alternatives. • Recommend a plan of action.

3.2.1 Understand the Context

The problem of providing sufficient cyber resiliency properties and behaviors is inherently situated in a programmatic, operational, architectural, and threat context. This step is intended to ensure that the context is sufficiently understood and that cyber resiliency constructs can be interpreted in that context, the relative priorities of cyber resiliency objectives can be assessed, and the applicability of cyber resiliency design principles, techniques, and approaches can be determined. The activities in this step can and should be integrated into activities under the Technical Management Processes in [SP 800-160 v1] and the Prepare and Categorize steps of the RMF [SP 800-37].

3.2.1.1 Identify the Programmatic Context

The programmatic context identifies how the system-of-interest is being acquired, developed, modified, or repurposed, including the life cycle stage, life cycle model, or system development approach (e.g., spiral, waterfall, agile, DevOps). Identification of the life cycle stage, life cycle model, and system development approach enables maturity as a consideration in defining cyber resiliency solutions. The programmatic context also identifies the stakeholders for the system-of-interest, the roles and responsibilities related to the system-of-interest, and the entities (organizations, organizational units, or individuals) in those roles.

In particular, the programmatic context identifies the entities responsible for directing, executing, and determining the acceptability of the results of engineering efforts related to the system (e.g., program office, systems engineer, systems integrator, authorizing official, and mission or business function owner). Each of these key stakeholders has a risk management strategy focused on different potential risks (e.g., cost, schedule, and technical or performance risks for a program office or systems engineer; security risks for an authorizing official; mission or business risks for a mission or business function owner). When these entities are part of the same organization, the risk management strategies for their respective areas of responsibility instantiate or are aligned with the organization's cyber risk management strategy.[39]

Technical or performance risks can include risks that quality properties (e.g., security, safety, system resilience, cyber resiliency) are insufficiently provided, as evidenced by the absence or poor execution of behaviors that should demonstrate those properties. The programmatic risk management strategy can reflect the relative priorities that other stakeholders—in particular,

[39] See Section 3.1.2.

the mission or business process owner and the authorizing official—assign to different quality properties. In addition, the programmatic risk management strategy can include constraints on less mature technologies, less commonly used products, or less commonly applied operational practices as part of managing technical or performance risks.[40]

In addition, other stakeholders may have their own risk management strategies or may be represented by an official within these entities (e.g., a system security officer to represent the security concerns of program managers whose proprietary information is handled by the system-of-interest) with a corresponding risk management strategy. An appreciation of the different risk management strategies (i.e., how the various stakeholders frame risk, including what threats and potential harms or adverse consequences are of concern to them, what their risk tolerances are, and what risk trade-offs they are willing to make) will enable the threat model to be defined and cyber resiliency constructs to be interpreted and prioritized in subsequent steps.

The programmatic context is not static. Technical, schedule, or security risks can include risks related to other programs or initiatives within the organization, its partners, or its suppliers. The design of the system-of-interest could assume successful completion of milestones by other programs or initiatives prior to a step in its development, contributing to technical or schedule risks. Schedule slips or failures to meet specific requirements by other programs or initiatives could also increase the attack surface of the system-of-interest or make it more fragile. Thus, understanding which other programs or initiatives could affect the system-of-interest is part of identifying the programmatic context.[41]

Identification of the programmatic context highlights the aspects of the programmatic risk management strategy that constrain possible solutions. One aspect is the relative priority of such quality attributes as safety, security, reliability, maintainability, system resilience, and cyber resiliency. Another is the relative preference for operational changes versus technical changes. Depending on the life cycle stage and the programmatic risk management strategy, changes to operational processes and procedures may be preferred to technical changes to the system.

3.2.1.2 Identify the Architectural Context

The architectural context identifies the type of system; its architecture or architectural patterns, if already defined; and its interfaces with or dependencies on other systems with consideration of whether it is (or is intended to be) part of a larger system-of-systems or a participant in a larger ecosystem. Key technologies, technical standards, or products included (or expected to be included) in the system are identified. Depending on the life cycle stage, identification of the architectural context can also include system locations, sub-systems or components, or layers in the architecture where cyber resiliency solutions could be applied. If this information is not yet available, it will be developed in a subsequent step.[42]

[40] See Section 3.1.8.

[41] See Section 2.3.

[42] See Section 3.2.3.3.

Identification of the type of system begins with identification of its general type (e.g., CPS,[43] application, enterprise service, common infrastructure as part of enterprise IT [EIT] or a large-scale processing environment [LSPE], EIT as a whole, or LSPE as a whole). The type of system determines which cyber resiliency techniques and approaches are most relevant.[44] Each type of system has an associated set of architectural patterns. For example, a CPS device typically includes a sensor, a controller (which is present in cyberspace), an actuator, and a physical layer; EIT typically includes enterprise services (e.g., identity and access management, mirroring and backup, email), common infrastructures (e.g., an internal communications network, a storage area network, a virtualization or cloud infrastructure), a demilitarized zone (DMZ) for interfacing with the Internet, and a collection of enterprise applications.

Identification of other systems with which the system-of-interest interfaces or on which it depends includes consideration of federation, networking, and scope. Federation typically restricts the set of solutions that can be applied and the metrics that can be defined and used since different system owners may be unwilling or unable to use the same technologies or share certain types or forms of information. Some systems are designed to operate without a network connection, at least transiently and often normally. The cyber resiliency solutions and means of assessing system cyber resiliency or solution effectiveness will be limited by whether the system is operating in detached mode. Depending on the programmatic context, the scope of "other systems" can include those constituting the system's development, test, or maintenance environment.

3.2.1.3 Identify the Operational Context

The operational context identifies how the system-of-interest is used or will be used (i.e., its usage context, which is closely related to the architectural context), how it will be administered and maintained (i.e., its support context, which is closely related to the programmatic and architectural contexts), how it interacts with or depends on other systems (i.e., its dependency context), and how usage and dependencies change depending on the time or circumstances (i.e., its temporal context).

The *usage context* identifies the primary mission or business functions that the system supports, any secondary or supporting missions or business functions, and the criticality and reliability with which the missions or business functions are to be achieved. Thus, the usage context can:

- Describe the system in terms of its intended uses, which include not only its primary mission or business function but also secondary or likely additional uses. The description includes identification of external interfaces—to networks, other supporting infrastructures and services, and end users—in a functional sense, keeping in mind that these interfaces can vary.
- Describe the system's criticality to its missions, stakeholders, end users, or the general public. Criticality is "an attribute assigned to an asset that reflects its relative importance or necessity in achieving or contributing to the achievement of stated goals" [SP 800-160 v1] and relates strongly to the potential impacts of system malfunction, degraded or denied

[43] Multiple levels of aggregation have been defined for CPS: a device, a system, or a system-of-systems [CPSPWG16]. For example, a smart meter is an example of a CPS device; a vehicle is an example of a CPS; and the Smart Grid is an example of a system-of-systems CPS.

[44] See Section 3.1.3.

performance, or not performing to the missions it supports, human life or safety, national security, or economic security (e.g., as in the context of critical infrastructure [NIST CSF]).

- Identify whether the system is or contains high-value assets (HVAs) (e.g., as defined in [OMB M-19-03], repositories of large volumes of PII or financial assets) or plays a central role (even if non-critical) in a critical infrastructure sector (e.g., financial services, Defense Industrial Base [DIB]) since these characteristics could attract specific types of adversaries.
- If possible, identify measures of effectiveness (MOEs) and measures of performance (MOPs) for organizational missions or business functions. Cyber resiliency effectiveness metrics, which can be defined and used later in the analysis process,[45] can sometimes repurpose mission MOEs, MOPs, or data collected to evaluate MOEs and MOPs and can often be related to MOEs and MOPs, particularly for cyber resiliency metrics related to Withstand or Recover.

The usage context also provides a general characterization of the system user population, including its size, scope, and assumed user awareness of and ability to respond to cyber threats. The usage context also indicates whether cyber defenders are actively involved in monitoring the system and responding to indications and warnings (I&W) of adverse conditions or behaviors.

The *support context* similarly provides a general characterization of the administrative and maintenance population, describes how system maintenance or updates are performed, and describes operational restrictions on maintenance activities or updates. For example, updates to embedded control units (ECUs) in a vehicle should be disallowed when driving. These aspects of the operational context determine the extent to which procedural solutions can be applied to the system-of-interest.

The *dependency context* identifies adjacent systems (i.e., systems with which the system-of-interest is connected); describes the types of information received from, supplied to, or exchanged with those systems; and identifies the criticality of the information connection to the system-of-interest and to the mission or business functions it supports. The dependency context also identifies infrastructures on which the system-of-interest depends (e.g., networks, power suppliers, and environmental control systems). These aspects of the operational context are used to bound the scope of the analysis (e.g., whether and for which adjacent or infrastructure systems changes are in scope, whether characteristics and behavior of these systems can be investigated or must be assumed). If the system-of-interest is part of a larger system-of-systems or is a participant in a larger ecosystem, the dependency context also identifies the implications of aggregation or federation for governance, system administration, and information sharing with other organizations or systems.

The *temporal context* identifies whether and how the usage and dependency contexts can change, depending on whether the system is operating under normal, stressed, or maintenance conditions; whether the system is being used for one of its secondary purposes; and how the system's usage and dependencies change over the course of executing mission or business functions.

[45] See Section 3.2.2.3 and Section 3.2.4.3.

Information about the support and dependency contexts can be used at this point in the analysis to characterize and subsequently identify the system's attack surfaces.[46] The operational context can be communicated by defining a motivating operational scenario or a small set of operational scenarios.

3.2.1.4 Identify the Threat Context

The threat context identifies threat sources, threat events, and threat scenarios of concern for the system-of-interest. In particular, the threat context helps to identify the characteristics and behaviors of adversaries whose attacks would necessarily undermine the system's ability to execute or support its missions, as well as the characteristics of relevant non-adversarial threats. Adversaries can include insiders as well as individuals or groups located outside of the system's physical and logical security perimeter. Adversary goals are identified and translated into cyber and mission effects. Adversary behaviors (i.e., threat events, attack scenarios, or TTPs) are also identified.

The threat context can:

- Identify the types of threats considered in programmatic or organizational risk framing. In addition to adversarial threats, these can include non-adversarial threats of human error, faults and failures, and natural disasters. A cyber resiliency analysis can identify scenarios in which adversaries can take advantage of the consequences of non-adversarial threat events.
- Identify the adversary's characteristics, to construct an adversary profile. Characteristics can include the adversary's ultimate goals and intended cyber effects, the specific time frame over which the adversary operates, the adversary's persistence (or, alternately, how easily the adversary can be deterred, discouraged, or redirected to a different target), the adversary's concern for stealth, and the adversary's targeting, which relates to the scope or scale of the effects that the adversary intends to achieve. Note that multiple adversaries can be profiled.
- Identify the types of threat events or adversarial behaviors of concern. Behaviors are described in terms of adversary TTPs and can be categorized using the categories of the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework [Strom17] or .govCAR [DHSCDM].
- Identify the representative attack scenarios of concern, describing each scenario with a phrase or a sentence. A set of general attack scenarios (e.g., as identified in [Bodeau18a] [Bodeau16]) can serve as a starting point. The attack scenarios of concern in the cyber resiliency use case should be clearly related to the system's mission. Note that a cyber resiliency analysis can focus on a single attack scenario or consider a set of scenarios.

A threat model can also include representative threat scenarios related to non-adversarial threat sources. For these, the scope or scale of effects, duration or time frame, and types of assets affected are identified. If possible, provide a reference to a publicly available description of a similar scenario to serve as an anchoring example.

Depending on its scope and purpose, a cyber resiliency analysis can focus on a single threat scenario. For example, a cyber resiliency analysis can be motivated by a publicized incident with

[46] See Section 3.2.3.1.

the purpose of the analysis being to determine the extent to which a particular system, mission or business function, or organization could be affected by a similar incident.

3.2.1.5 Interpret and Prioritize Cyber Resiliency Constructs

To ensure that cyber resiliency concepts and constructs are meaningful in the identified contexts, one or more of the following sub-tasks can be performed:

- Restate and prioritize cyber resiliency objectives[47] and sub-objectives.[48] Identify, restate, and prioritize capabilities or activities that are needed to achieve relevant sub-objectives in light of the identified threat context. These constructs are restated in terms that are meaningful in the architectural and operational contexts and prioritized based on programmatic considerations and stakeholder concerns. Note that responsibility for some capabilities or activities may be allocated to system elements outside of the scope of the engineering or risk management decisions that the cyber resiliency analysis is intended to support.
- Determine the potential applicability of cyber resiliency design principles. This involves considering organizational and programmatic risk management strategies to determine which strategic design principles may apply. It also involves considering the architecture, operational context, and threat environment to identify the relevance of structural design principles to this situation. Relevant structural design principles are restated in situation-specific terms (e.g., in terms of the technologies that are part of the system).
- Determine the potential applicability of cyber resiliency techniques and (depending on the level of detail with which the architectural context is defined) implementation approaches. This involves considering the architecture, operational context, and threat context. The relevance of the techniques and approaches to this situation is described and assessed. Relevant techniques and approaches can be restated and described in terms of architectural elements (e.g., allocating an implementation approach to a specific system element or identifying an architectural layer at which a technique can be applied). However, detailed descriptions are generally deferred to a later stage in a cyber resiliency analysis.[49]

The determination that some cyber resiliency constructs are not applicable, based on the considerations discussed in Section 3.1, narrows the focus of subsequent steps in the cyber resiliency analysis, which saves work and increases the usefulness of the results.

3.2.2 Develop the Cyber Resiliency Baseline

In order to determine whether cyber resiliency improvement is needed, the baseline for the system (as it is understood at the stage in the life cycle when the cyber resiliency analysis is performed) must be established.

3.2.2.1 Establish the Initial Cyber Resiliency Baseline

As discussed in Section 3.1.5.1, a system reflects architectural and design decisions and investments in specific technologies and products motivated by other specialty engineering

[47] See Section 3.1.1.

[48] See Appendix D, Table D-1.

[49] See Section 3.2.3.3.

disciplines. Capabilities are identified from such functional areas as COOP and contingency planning; security, cybersecurity, and cyber defense; performance management; reliability, maintainability, and availability (RMA); safety; and survivability. Identification of capabilities can involve decomposition of the system-of-interest into constituent sub-systems, functional areas, and/or architectural locations.[50]

Capabilities can be characterized in terms of the cyber resiliency techniques and approaches they can implement and/or the cyber resiliency design principles they can be used to apply. Capabilities can also be characterized in terms of how easily their configuration or operational use can be adapted to address specific cyber resiliency concerns, how dynamically they can be reconfigured or repurposed, and how compatible they are with other cyber resiliency techniques and approaches (e.g., deception, unpredictability).

3.2.2.2 Identify Gaps and Issues

Depending on the life cycle stage, issues may already be tracked, or it may be possible to identify gaps in required capabilities and issues with the system's design, implementation, or use. Such information can be found in after-action reports from exercises, penetration test reports, incident reports, and reporting related to ongoing assessments and ongoing risk response actions (RMF tasks M-2 and M-3) [SP 800-37]. Security gaps may also have been identified from a coverage analysis with respect to a taxonomy of attack events or TTPs [DHSCDM].

Because senior leadership is often aware of issues and gaps, recommended cyber resiliency solutions will need to be characterized in terms of how and how well the solutions address the issues and gaps, as well as in terms of other benefits that the recommended solutions provide (e.g., improved stability, improved performance).

3.2.2.3 Define Evaluation Criteria and Make Initial Assessment

One or more evaluation criteria are established and used to make an initial assessment. Cyber resiliency can be evaluated in multiple ways, including:

- How well the system achieves (or, assuming it meets its requirements, will achieve) cyber resiliency objectives and sub-objectives (considering the priority weighting established earlier),[51] can provide capabilities, or perform activities supporting achievement of cyber resiliency objectives. An initial assessment can be expressed as high-level qualitative assessments (e.g., on a scale from Very Low to Very High) for the cyber resiliency objectives and subsequently refined based on analysis of the system. An initial assessment can also take the form of a cyber resiliency coverage map, indicating whether and how well the relevant cyber resiliency constructs that were determined to be relevant have been applied.[52] Alternately (if the information is available) or subsequently (based on the analysis described in Section 3.2.3.1 and Section 3.2.3.3),[53] this assessment can be expressed as a cyber resiliency score.

[50] See Section 3.1.6.

[51] See Section 3.2.1.5.

[52] See Section 3.2.1.5.

[53] See Section 3.2.4.3.

- How well the system's capabilities cover (i.e., have at least one effect on) adversary activities as identified by the threat context.[54] This can be expressed as a threat heat map [DHSCDM] or a simple threat coverage score. For an initial assessment, coverage can be in terms of attack stages.[55] Alternately or subsequently, a more nuanced threat coverage score based on the organization's risk management strategy can be computed using the relative priorities of the general types of effects (e.g., increase adversary cost, decrease adversary benefits, increase adversary risk) and of the specific effects (e.g., redirect, preclude, impede, detect, limit, expose) if the risk management strategy establishes such priorities.
- The level of cyber risk in terms of risk to missions, business functions, or other forms of risk (e.g., security, safety, reputation). An assessment of this form is possible if the organization has established a risk model, or at least a consequence model, for such forms of risk. An initial assessment will typically rely on an existing security risk assessment [SP 800-30].
- The level of operational resilience (i.e., mission or business function resilience) in terms of functional performance measures under stress. An assessment of this form is possible if the organization has established such performance measures. An initial assessment will typically rely on an existing performance assessment, which describes operational resilience in the face of prior incidents and will be subject to uncertainty since prior incidents may be poor predictors of future ones.

Additional evaluation criteria can consider how well the system meets its security requirements or achieves its security objectives and how well the system satisfies its mission or business function requirements. While such evaluations are independent of cyber resiliency analysis, they can form part of the baseline against which potential solutions can be evaluated.

Stakeholder concerns and priorities are used to determine which (or which combination) of these will be used to evaluate alternative solutions. Approaches to assessment (e.g., scoring systems, qualitative assessment scales, metrics and measures of effectiveness) and candidate metrics can be identified for use in subsequent steps. In addition, evaluation criteria can involve assessments of potential costs in terms of financial investment over subsequent life cycle stages (e.g., acquiring, integrating, operating, and maintaining a cyber resiliency solution), opportunity costs (e.g., constraints on future engineering decisions or system uses), and increased programmatic risk (e.g., potential cost risk, schedule impacts, performance impacts).

3.2.3 Analyze the System

In this step, the system is analyzed in its operational context from two perspectives. First, a mission or business function perspective is applied to identify critical resources (i.e., those resources for which damage or destruction would severely impact operations) and sources of system fragility. Second, an adversarial perspective is applied to identify high-value primary and secondary targets of APT actors [OMB M-19-03] and develop representative attack scenarios. Based on this analysis and the results of the previous baseline assessment, opportunities for improvement are identified.

[54] See Appendix F.

[55] See Section F.2.

3.2.3.1 Identify Critical Resources, Sources of Fragility, and Attack Surfaces

A critical resource can be a resource for which damage (e.g., corruption or reduced availability), denial of service, or destruction results in the inability to complete a critical task. In addition, if a resource is used in multiple tasks, it can be highly critical overall even if it is not critical to any of those functions individually if its damage, denial, or destruction results in a delay for a time-critical mission or business function. Critical resources can be identified using a variety of methods specific to contingency planning, resilience engineering, and mission assurance. These include Criticality Analysis [IR 8179], Mission Impact Analysis (MIA), Business Impact Analysis (BIA) [SP 800-34], Crown Jewels Analysis (CJA), and cyber mission impact analysis (CMIA).

For cyber resiliency analysis, the identification of critical resources is based on an understanding of functional flows or of mission or business function threads. A resource can be highly critical at one point in a functional flow or a mission thread and of very low criticality at other points. A functional flow analysis or a mission thread analysis can reveal such time dependencies.

Systems can also be analyzed to identify sources of fragility or brittleness. While identification of single points of failure is a result of the analysis methods mentioned above, network analysis or graph analysis (i.e., analysis of which system elements are connected, how and how tightly the system elements are connected, and whether some sets of system elements are more central) can determine whether the system is fragile (i.e., whether it will break if a stress beyond a well-defined set is applied). Similarly, graphical analysis of the distribution of different types of components can help determine how easily a given stress (e.g., exploitation of a zero-day vulnerability) could propagate.

Finally, the attack surfaces to which cyber resiliency solutions can be applied can be identified. Information about the programmatic, architectural, and operational context determines which attack surfaces are within the scope of potential cyber resiliency solutions. For example, if the programmatic context determines support systems to be in scope, those systems are an attack surface in addition to the interfaces and procedures by which updates are made to the system-of-interest; if the system-of-interest is an enterprise service (architectural context), its interfaces to other services on which it depends as well as to applications which use it are also attack surfaces; if the system has users (operational context), the user community is an attack surface.[56]

3.2.3.2 Represent the Adversary Perspective

As described in Section 3.2.1, cyber resiliency analysis assumes an architectural, operational, and threat context for the system being analyzed. These contextual assumptions provide the starting point for a more detailed analysis of how an adversary could adversely affect the system and thereby cause harm to the mission or business functions it supports, the organization, individuals for whom the system handles PII or whose safety depends on the system, or the environment. The attack scenarios of concern that were identified as part of the threat context serve as a starting point.[57] Depending on the scope of the analysis,[58] these attack scenarios can

[56] See Section D.5.1.3.

[57] See Section 3.2.1.4.

[58] As noted in Section 3.2.1.4, a cyber resiliency analysis can be focused on a single attack scenario.

be complemented by scenarios driven by adversary goals, scenarios targeting critical assets or high-value assets,[59] or scenarios that take advantage of sources of fragility.

The adversary perspective (i.e., what harm can be done, how easily, and at what cost to the attacker) can be represented in different ways, depending on the stage of the system life cycle and the corresponding level and amount of information about the system architecture, design, implementation, and operations. At a minimum, an attack scenario can identify stages in the attack (e.g., administer, engage, persist, cause effect, and maintain ongoing presence), the adversary objectives or categories of TTPs at each stage (e.g., reconnaissance, exploitation, lateral movement, denial), and the system elements compromised in each stage. Depending on the system life cycle stage, it may be possible to identify individual TTPs (e.g., pass the hash) or examples of specific malware.[60]

Attack scenarios can be represented as part of a model-based engineering effort; using attack tree or attack graph analysis; in terms of fault tree analysis or failure modes, effects, and criticality analysis (FMECA); or based on the identification of loss scenarios from System-Theoretic Process Analysis (STPA). Common elements across the attack scenarios (e.g., recurring adversary TTPs) can be starting points for identifying potential alternative solutions.

Depending on the scope of the cyber resiliency analysis, attack scenarios can be developed that target supporting systems. Such attack scenarios may be the result of a supply chain risk analysis or a cyber resiliency or cybersecurity analysis of systems or organizations responsible for development, integration, testing, or maintenance.

3.2.3.3 Identify and Prioritize Opportunities for Improvement

The identification of potential areas of improvement typically relies on the interpretation and prioritization of cyber resiliency constructs performed earlier.[61] Potential cyber resiliency techniques or implementation approaches can be identified in system-specific terms, mapped to system elements or architectural layers, and stated as desired improvements to system elements or to the system as a whole. Desired improvements are prioritized based on how and how well they are expected to reduce risks as identified by stakeholders.[62]

In more detail, this task in the analysis process can include the following sub-tasks:

- Identify potentially applicable techniques or approaches. If the set of potentially applicable techniques and approaches has already been identified,[63] it can be narrowed by identifying the set of techniques and approaches related to prioritized objectives using Appendix D, Table D-13 or to potentially applicable structural design principles using Table D-15. (If only the applicable strategic design principles were identified, Table D-14 can be used to identify relevant objectives and Table D-10 can be used to identify relevant structural design principles.) Otherwise, the set of techniques and approaches related to prioritized

[59] See OMB M-19-03.

[60] However, specific malware should be treated as a motivating example only. Cyber resiliency engineering assumes that unforeseen malware can be used and seeks to mitigate types of adversary actions.

[61] See Section 3.2.1.5.

[62] See Section 3.2.1.1.

[63] See Section 3.2.1.5.

objectives or structural design principles can be refined by taking the architectural and programmatic context into consideration. The potentially applicable techniques or approaches are described in system-specific terms.

- Identify locations where cyber resiliency solutions could be applied.[64] The set of locations (i.e., sub-systems or components, layers in the architecture, or interfaces between sub-systems or between layers) where cyber resiliency solutions could be applied is determined by the system architecture as constrained by context.[65] For example, the programmatic context may prioritize cyber resiliency solutions that change how existing technologies are used over changes to the system architecture (e.g., replacing specific system elements); the architectural context may restrict locations to specific interfaces (e.g., if the system-of-interest is an enterprise service, solutions may be applied to its interfaces with sub-systems or applications which use it or with supporting services, particularly security services); or the operational context may constrain the extent to which new user procedures can be made part of the system (e.g., depending on the size of, cyber expertise of, or organizational control over the user population).
- Identify desired improvements to system elements or to the system-of-interest as a whole. Statements of desired improvements described in terms specific to the architectural and operational context can be more meaningful to stakeholders than general statements about improved use of a cyber resiliency technique or a more effective application of a cyber resiliency design principle. Potential improvements can be described in terms of improved protection for critical resources, reduced fragility, or the ability to address threats more effectively.
- Prioritize desired improvements using the identified evaluation criteria (e.g., improve the ability of a given system element to continue functioning by enabling that element to be dynamically isolated, decrease adversary benefits by reducing the concentration of highly-sensitive information in a single asset, or reduce mission risks by providing extra resources for high-criticality tasks).

3.2.4 Define and Analyze Specific Alternatives

In this step, specific ways to make desired improvements (i.e., architectural changes, ways to implement cyber resiliency techniques in the context of the existing architecture, ways to use existing system capabilities more effectively to improve resilience) are identified and analyzed in terms of potential effectiveness. These specific alternatives form a solution set, which will be used in the final step to construct potential courses of action.

3.2.4.1 Define Potential Technical and Procedural Solutions

Potential applications of cyber resiliency techniques and implementation approaches to the system-of-interest in its environment of operations in order to provide one or more desired improvements are identified.[66] These applications (i.e., potential solutions to the problem of improving mission or operational resilience by improving cyber resiliency) can be purely technical, purely procedural, or combinations of the two.

[64] See Section 3.1.6.

[65] See Section 3.2.1.

[66] See Section 3.2.3.3.

Potential solutions can incorporate or build on investments from other disciplines.[67] The set of technologies and products that are available at some level of maturity[68] for incorporation into the system depends on the type of the system.[69] The degree to which relatively immature technologies can be considered depends on the programmatic risk management strategy.[70]

The level of detail with which a potential solution is described depends on how specifically the context was described in the first step.[71] In particular, if the architectural and operational contexts were described in general terms, potential solutions will necessarily be described at a high-level. On the other hand, if the cyber resiliency analysis is being performed for an existing system, a potential solution can be described in terms of specific technologies or products to be integrated into the system, where in the system those technologies will be used, how they will interface with other system elements, configuration settings or ranges of settings for products, and processes or procedures to make effective use of existing or newly acquired technologies.

The description of a potential solution can include identification of the gaps it is expected to address,[72] the threats (e.g., attack scenarios, adversary objectives or categories of TTPs, or adversary actions) it is intended to address,[73] or the reduced exposure of critical resources, sources of fragility, or attack surfaces to threats.[74] These different elements of a potential solution's description can be used to evaluate the solution.[75]

3.2.4.2 Define Potential Solutions for Supporting Systems and Processes

If programmatic and operational contexts support improvements to supporting systems and processes, the potential applications of cyber resiliency techniques and approaches to these systems and processes are also identified. Such applications can include modifications to contracting to help ensure that controlled unclassified information (CUI) or other sensitive information is protected [SP 800-171], improvements to supply chain risk management (SCRM) as determined by SCRM analysis [SP 800-161], and restrictions on or re-architecting of system development, testing, or maintenance environments to improve the cyber resiliency of those environments.

3.2.4.3 Analyze Potential Solutions with Respect to Criteria

Potential solutions can be analyzed with respect to one or more criteria.[76] Evaluation can employ qualitative or semi-quantitative assessments (using subject matter expert [SME] judgments) or quantitative metrics (evaluated in a model-based environment, laboratory, cyber range, or test environment; metrics to support analysis of alternatives are typically not

[67] See Section 3.1.5.
[68] See Section 3.1.8.
[69] See Section 3.1.3.
[70] See Section 2.3 and Section 3.2.1.1.
[71] See Section 3.2.1.
[72] See Section 3.2.2.2.
[73] See Section 3.2.3.2.
[74] See Section 3.2.3.1.
[75] See Section 3.2.4.3.
[76] See Section 3.2.2.3.

evaluated in an operational environment). Potential solutions can be analyzed to determine, for example:

- How much the solution could improve the ability of the system to achieve its (priority-weighted) cyber resiliency objectives or sub-objectives. This can be expressed as a change in a cyber resiliency score or as a coverage map for the relevant cyber resiliency constructs. Alternately or in support of scoring, performance metrics for activities or capabilities related to cyber resiliency sub-objectives can be evaluated.
- How well the system, with the solution applied, addresses adversary activities or attack scenarios as identified by the threat context. As noted in Section 3.2.2.3, this can take the form of a threat heat map or a threat coverage score using a taxonomy of adversary activities (e.g., [MITRE18]). It can also take the form of an adversary return on investment (ROI) score or a more nuanced threat coverage score.[77] Alternately or in support of scoring, performance metrics for specific types of effects on adversary actions can be defined and evaluated before and after the solution is applied (e.g., length of time it takes an adversary to move laterally across a system or an enclave).
- How much the solution could improve the system's coverage of adversary TTPs using capabilities defined in [NIST CSF]. This can be expressed as a change in a score or using a threat heat map [DHSCDM].
- How much the solution could decrease the level of cyber risk or a specific component of risk (e.g., level of consequence). As discussed in Appendix F,[78] effects on adversary activities have associated effects on risk.
- How much the solution could improve the level of operational resilience in terms of functional performance measures under stress. As discussed in Section D.5.1, some strategic design principles for cyber resiliency are closely related to design principles for Resilience Engineering. Thus, a solution that applies one or more of those design principles can be expected to improve resilience against non-adversarial as well as adversarial threats.
- Whether and how much the solution could improve the system's ability to meet its security requirements. Evaluation with respect to this criterion can involve qualitative assessments by subject matter experts (SME), an explanatory description, a list of previously unmet requirements that the solution can help meet, or specific security performance metrics that can be evaluated before and after the solution is applied.
- Whether and how much the solution could improve the system's ability to meet its mission or business function performance requirements. Similar to a security requirements criterion, evaluation with respect to this criterion can involve an explanatory description, qualitative assessments by SMEs, a list of previously unmet requirements that the solution can help meet, or specific functional performance metrics that can be evaluated before and after the solution is applied.

In addition, the potential costs of a solution can be identified or assessed. The product of this step is a list of alternative solutions, with each alternative characterized (e.g., using a coverage map or a description) or assessed with respect to the identified criteria.

[77] See Appendix F.

[78] See Table F-1.

3.2.5 Develop Recommendations

Unless the scope of the cyber resiliency analysis is narrow, the number and variety of potential solutions may be large. Sets of potential solutions that could be implemented at the same time can be constructed and analyzed to ensure compatibility, identify possible synergies, and determine whether specific solutions should be applied sequentially rather than simultaneously. In addition, programmatic and operational risks associated with alternative solutions can be identified. The result of this step is a recommended plan of action.

3.2.5.1 Identify and Analyze Alternatives

One or more alternatives (i.e., sets of potential solutions that could be implemented at the same time or sequentially such as in successive spirals) can be identified using either total cost or a requirement for a consistent level of maturity[79] (e.g., requiring all technical solutions in the set to be available as commercial products by a specific milestone) to bound each set. Where possible, a set of potential solutions should be defined to take advantage of synergies (as discussed in Section 3.1.4 and identified in Appendix D, Table D-3). At a minimum, each set should be analyzed to ensure that there are no internal conflicts. If the solutions in a set are to be implemented sequentially, functional dependencies among those solutions should be identified. In addition, functional dependencies on other system elements (particularly those involving investments due to other disciplines)[80] should be identified since changes in system elements can be made for a variety of reasons. Finally, functional dependencies on other organizational efforts (e.g., programs, initiatives) should be identified to ensure that changes to the attack surfaces of the system-of-interest, the organization's infrastructure and supporting services, and other systems or assets are understood and the associated risks managed.[81]

3.2.5.2 Assess Alternatives

Each alternative can be assessed or characterized in terms of the evaluation criteria.[82] To support assessments, the adversarial analysis[83] can be revisited for each alternative. Due to synergies or other interactions between cyber resiliency techniques, changes in scores, heat maps, or coverage maps must be determined by analysis rather than by simply combining previously determined values. In addition, each alternative should be analyzed to determine whether it makes new attack scenarios (or non-adversarial threat scenarios) possible. If it does, those scenarios should be analyzed to determine whether changes should be made to the alternative.

Each alternative can also be described in terms of the issues it resolves, the gaps it fills,[84] or whether it provides improved protection for critical resources, reduced fragility, or the ability to address threats more effectively. Finally, each alternative can be assessed or described in terms of its effects on programmatic risk (e.g., total costs, changes to schedule risk, changes to technical or performance risk) or other risks of concern to stakeholders. If an alternative

[79] See Section 3.1.8.

[80] See Section 3.1.5.

[81] See Section 2.3.

[82] See Section 3.2.4.3.

[83] See Section 3.2.3.2.

[84] See Section 3.2.2.2.

diverges from the risk management strategies of one or more stakeholders, this divergence should be noted so that a compensating risk management approach can be made part of the recommendation if the alternative is in fact recommended.

3.2.5.3 Recommend a Plan of Action

A recommended plan of action resulting from a cyber resiliency analysis can take the form of a set of selected alternatives to be implemented in successive phases. For each phase, the costs, benefits, and risk management approaches can be identified, accompanied by identification of circumstances which could indicate the need to revisit the recommendations. However, as noted in Section 3.1, a cyber resiliency analysis can be narrowly focused. If this is the case, the recommendations resulting from the analysis will take a form directed by the focus of the analysis.

CYBER RESILIENCY ENGINEERING

A COMPLEMENT TO OTHER SPECIALTY ENGINEERING DISCIPLINES

As presented in this publication, cyber resiliency engineering is a specialty systems engineering discipline, based on the recognition that (1) mission and business functions depend on systems which include or depend on cyber resources, (2) advanced persistent threat (APT) actors can establish and maintain a covert presence in systems, particularly by compromising cyber resources, and (3) essential organizational missions and business functions must be assured despite the activities of APT actors. The cyber resiliency engineering framework presented in Section 2.1 and the tailorable process for cyber resiliency analysis presented in Section 3.2 are motivated by that recognition. As discussed in those sections and in Section C.3, cyber resiliency engineering draws from, is aligned with, and can support other specialty systems engineering disciplines.

The cyber resiliency goals, objectives, techniques, and design principles, as well as many of the implementation approaches, are defined in technology-neutral terms. This is deliberate, to facilitate alignment with frameworks for other specialty systems engineering disciplines. The representative examples of these constructs are specific to systems which include cyber resources. The selection of the objectives, techniques, design principles, and approaches for inclusion in the cyber resiliency engineering framework is motivated by practical experience with engineering systems with requirements for mission assurance in the face of APT activities, by landscape surveys of existing and emerging technologies and practices for meeting those requirements, and by surveys of various research strategies. The expectation is that the set of representative examples will continue to grow and change, possibly leading to changes in the set of implementation approaches, as technologies and practices for integrating cyber resources into systems continue to evolve.

REFERENCES

LAWS, POLICIES, DIRECTIVES, REGULATIONS, STANDARDS, AND GUIDELINES

LAWS AND EXECUTIVE ORDERS	
[FISMA]	Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.govinfo.gov/app/details/PLAW-113publ283
[FOIA96]	Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996. https://www.govinfo.gov/app/details/PLAW-104publ231
[EO 13800]	Executive Order 13800 (2017), Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. (The White House, Washington, DC), DCPD-201700327, May 11, 2017. https://www.govinfo.gov/app/details/DCPD-201700327
[EO 14028]	Executive Order 14028 (2021), Improving the Nation's Cybersecurity. (The White House, Washington, DC), May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity
REGULATIONS, DIRECTIVES, INSTRUCTIONS, PLANS, AND POLICIES	
[OMB A-130]	Office of Management and Budget (2016) Managing Information as a Strategic Resource (The White House, Washington, DC), OMB Circular A-130, July 2016. Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
[CNSSI 1253]	Committee on National Security Systems (2014) Security Categorization and Control Selection for National Security Systems. (National Security Agency, Fort George G. Meade, MD), CNSS Instruction 1253. Available at https://www.cnss.gov/CNSS/openDoc.cfm?HSjOTWr2HMkv0zk2nLvB8A==
[CNSSI 4009]	Committee on National Security Systems (2015) Committee on National Security Systems (CNSS) Glossary. (National Security Agency, Fort George G. Meade, MD), CNSS Instruction 4009. Available at https://www.cnss.gov/CNSS/openDoc.cfm?pR8Egv4JDxhquaRPbbdq8A==
[HSPD23]	National Security Presidential Directive/NSPD-54 Homeland Security Presidential Directive/HSPD-23, Cybersecurity Policy, January 2008.
[OMB M-19-03]	Office of Management and Budget (2018) Management of High Value Assets. (The White House, Washington, DC), OMB Memorandum M-19-03, December 2018. Available at https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf
[PPD8]	Presidential Policy Directive (PPD) 8, *National Preparedness*, March 2011, last published August 2018. Available at https://www.dhs.gov/presidential-policy-directive-8-national-preparedness
[FMRS20]	Federal Mission Resilience Strategy 2020, December 2020. Available at https://www.hsdl.org/?view&did=848323

[PPD21] Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Resilience,* February 2013. Available at https://www.dhs.gov/sites/default/files/publications/PPD-21-Critical-Infrastructure-and-Resilience-508.pdf

STANDARDS, GUIDELINES, AND REPORTS

[ISO 73] International Organization for Standardization (ISO) Guide 73:2009, *Risk management – Vocabulary*, November 2009. https://www.iso.org/standard/44651.html

[ISO 15288] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2015) *ISO/IEC/IEEE 15288:2015 – Systems and software engineering — Systems life cycle processes* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/63711.html

[ISO 24765] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2017) *ISO/IEC/IEEE 24765-2017 – Systems and software engineering — Vocabulary* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/71952.html

[FIPS 199] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

[SP 800-30] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[SP 800-34] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning Guide for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-34, Rev. 1, Includes updates as of November 11, 2010. https://doi.org/10.6028/NIST.SP.800-34r1

[SP 800-37] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[SP 800-39] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[SP 800-53] Joint Task Force Transformation Initiative (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[SP 800-53B] Joint Task Force Transformation Initiative (2019) Control Baselines for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53B. https://doi.org/10.6028/NIST.SP.800-53B

[SP 800-82] Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 2. https://doi.org/10.6028/NIST.SP.800-82r2

[SP 800-95] Singhal A, Winograd T, Scarfone KA (2007) Guide to Secure Web Services. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-95. https://doi.org/10.6028/NIST.SP.800-95

[SP 800-125B] Chandramouli R (2016) Secure Virtual Network Configuration for Virtual Machine (VM) Protection. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-125B. https://doi.org/10.6028/NIST.SP.800-125B

[SP 800-160 v1] Ross RS, Oren JC, McEvilley M (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018. https://doi.org/10.6028/NIST.SP.800-160v1

[SP 800-161] Boyens JM, Paulsen C, Moorthy R, Bartol N (2015) Supply Chain Risk Management Practices for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161. https://doi.org/10.6028/NIST.SP.800-161

[SP 800-171] Ross RS, Dempsey KL, Viscuso P, Riddle M, Guissanie G (2016) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171, Rev. 1, Includes updates as of June 7, 2018. https://doi.org/10.6028/NIST.SP.800-171r1

[SP 800-183] Voas, J (2016) Networks of 'Things'. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-183. https://doi.org/10.6028/NIST.SP.800-183

[SP 800-207] Rose S, Borchert O, Mitchell S, Connelly S (2019) Zero Trust Architecture. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-207. https://doi.org/10.6028/NIST.SP.800-207-draft

[SP 1500-201] Burns MJ, Greer C, Griffor ER, Wollman DA (2017) Framework for Cyber-Physical Systems: Volume 1, Overview, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1500-201. https://doi.org/10.6028/NIST.SP.1500-201

[SP 1190] Butry D, et. Al (2016) Community Resilience Planning Guide for Buildings and Infrastructure Systems, Volume I. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1190, Vol. 1. https://doi.org/10.6028/NIST.SP.1190v1

[IR 8179] Paulsen C, Boyens JM, Bartol N, Winkler K (2018) Criticality Analysis Process Model: Prioritizing Systems and Components. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8179. https://doi.org/10.6028/NIST.IR.8179

[IR 8202] Yaga DJ, Mell PM, Roby N, Scarfone KA (2018) Blockchain Technology Overview. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8202. https://doi.org/10.6028/NIST.IR.8202

[IR 8259] Fagan M, Megas KN, Scarfone KA, Smith M (2019) Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Interagency or Internal Report (IR) 8259. https://doi.org/10.6028/NIST.IR.8259-draft

[IR 8286] Stine K, Quinn S, Witte G, Gardner RK (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. https://doi.org/10.6028/NIST.IR.8286

[IR 8301] Lesavre L, Varin P, Yaga D (2021) Blockchain Networks: Token Design and Management Overview. National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Interagency or Internal Report (IR) 8301. https://doi.org/10.6028/NIST.IR.8301

[IR 8360] Hu VC (2021) Machine Learning for Access Control Policy Verification. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Interagency or Internal Report (IR) 8360. https://doi.org/10.6028/NIST.IR.8360-draft

[MIL-STD-882E] Department of Defense (2012) *MIL-STD-882E – Standard Practice: System Safety* (U.S. Department of Defense, Washington, DC). Available at https://www.dau.edu/cop/esoh/Pages/Topics/System%20Safety%20Methodology.aspx

MISCELLANEOUS PUBLICATIONS AND WEBSITES

[Avizienis04] Avižienis A, Laprie JC, Randell B (2004) Dependability and Its Threats: A Taxonomy. *Building the Information Society*, *IFIP International Federation for Information Processing*, ed Jacquart R (Springer, Boston, MA), Vol. 156, pp 91-120. https://doi.org/10.1007/978-1-4020-8157-6_13

[Bodeau11] Bodeau D, Graubart R (2011) Cyber Resiliency Engineering Framework, Version 1.0. https://www.mitre.org/sites/default/files/pdf/11_4436.pdf

[Bodeau15] Bodeau D, Graubart R, Heinbockel W, Laderman E (2015) Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques. (The MITRE Corporation, Bedford, MA), MITRE Technical Report MTR-140499R1. Available at http://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf

[Bodeau16] Bodeau D, Graubart R (2016) Cyber Prep 2.0: Motivating Organizational Cyber Strategies in Terms of Preparedness. (The MITRE Corporation, Bedford, MA), MITRE Technical Report MTR-150264. Available at https://www.mitre.org/sites/default/files/publications/15-0797-cyber-prep-2-motivating-organizational-cyber-strategies.pdf

[Bodeau17] Bodeau D, Graubart R (2017) Cyber Resiliency Design Principles: Selective Use Throughout the Life Cycle and in Conjunction with Related Disciplines. (The MITRE Corporation, Bedford, MA), MITRE Technical Report MTR-170001. Available at https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf

[Bodeau18a] Bodeau DJ, McCollum CD, Fox DB (2018) Cyber Threat Modeling: Survey, Assessment, and Representative Framework. (The MITRE Corporation, McLean, VA), PR 18-1174. Available at https://www.mitre.org/sites/default/files/publications/pr_18-1174-ngci-cyber-threat-modeling.pdf

[Bodeau18b] Bodeau D, Graubart R, McQuaid R, Woodill J (2018) Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods. (The MITRE Corporation, Bedford, MA), MITRE Technical Report MTR-180314. Available at https://www.mitre.org/sites/default/files/publications/pr-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf

[Bodeau21] Bodeau D, Graubart R, Jones LK, Laderman E (2021). Cyber Resiliency Approaches and Controls to Mitigate Adversary Tactics, Techniques, and Procedures (TTPs): Mapping Cyber Resiliency to the ATT&CK® Framework – Revision 1. (The MITRE Corporation, Bedford, MA), MITRE Technical Report MTR-200286R1.

[Brtis16] Brtis J (2016) How to Think about Resilience in a DoD Context. (The MITRE Corporation, Colorado Springs, CO), MITRE Technical Report MTR-160138.

[Clemen13] Clemen RT, Reilly T (2013) *Making Hard Decisions with the Decision Tools Suite* (South-Western Cengage Learning, Mason, OH), 3rd Ed., pp 848.

[CPSPWG16] Cyber-Physical Systems Public Working Group (2016) Framework for Cyber-Physical Systems, Release 1.0 (National Institute of Standards and Technology, Gaithersburg, MD). Available at https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf

[DHS10] Department of Homeland Security Risk Steering Committee (2010) DHS Risk Lexicon. (U.S. Department of Homeland Security, Washington, DC), 2010 Edition. Available at https://www.dhs.gov/sites/default/files/publications/dhs-risk-lexicon-2010_0.pdf

[DHSCDM] Department of Homeland Security, "CDM Program What is .govCAR?" https://www.cisa.gov/sites/default/files/publications/2020%2009%2003_%20CDM%20Program%20govCAR_Fact%20Sheet_2.pdf

[DOD15] Department of Defense, "Department of Defense Cybersecurity Test and Evaluation Guidebook, Version 2.0," April 2018. Available at https://www.dau.edu/cop/test/DAU%20Sponsored%20Documents/CSTE%20Guidebook%202.0_FINAL%20(25APR2018).pdf

[DOD16] Department of Defense (2016) Mission Assurance (U.S. Department of Defense, Washington, DC), DoD Directive (DODD) 3020.40. Available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040_dodd_2016.pdf

[DSB13] Defense Science Board (2013) Resilient Military Systems and the Advanced Cyber Threat. (U.S. Department of Defense, Washington, DC). Available at https://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf

[Folk15] Folk C, Hurley DC, Kaplow WK, Payne JF (2015) The Security Implications of the Internet of Things. (AFCEA International Cyber Committee). Available at https://www.afcea.org/site/sites/default/files/files/AFC_WhitePaper_Revised_Out.pdf

[GAO18] Government Accountability Office (2018) Weapon Systems Cybersecurity. (Government Accountability Office, Washington, DC), GAO-19-128, October 2018. Available at https://www.gao.gov/assets/700/694913.pdf

[Heckman15] Heckman KE, Stech FJ, Thomas RK, Schmoder B, Tsow AW (2015) Cyber Denial, Deception and Counter Deception: A Framework for Supporting Active Cyber Defense, *Advances in Information Security* (Springer, Cham, Switzerland), Vol. 63.

[Höller15] Höller A, Rauter T, Iber J, Kreiner C (2015) Towards Dynamic Software Diversity for Resilient Redundant Embedded Systems. *Proceedings of Software Engineering for Resilient Systems: 7th International Workshop, SERENE 2015* (Springer, Paris, France), pp 16-30. https://doi.org/10.1007/978-3-319-23129-7_2

[Hutchins11] Hutchins EM, Cloppert MJ, Amin RM (2011) Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, ed Ryan J (Academic Publishing International, Reading, UK), Vol. 1, pp 78-104.

[IEEE90] Institute of Electrical and Electronics Engineers (1990) *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*, (IEEE, New York, NY).

[IEEE17] Institute of Electrical and Electronics Engineers, Association for Computing Machinery (2017) *Enterprise IT Body of Knowledge – Glossary. Enterprise IT Body of Knowledge*. Available at http://eitbokwiki.org/Glossary#eit

[INCOSE11] International Council for Systems Engineering (2011) *Resilient Systems Working Group Charter*. (INCOSE, San Diego, CA).

[INCOSE14] International Council on Systems Engineering (2015) *System Engineering Handbook—A Guide for System Engineering Life Cycle Processes and Activities*. (John Wiley & Sons, Hoboken, NJ), 4th Ed.

[ISACA] ISACA (2019) *ISACA Glossary of Terms*. Available at https://www.isaca.org/pages/glossary.aspx

[Jackson07] Jackson S (2007) A Multidisciplinary Framework for Resilience to Disasters and Disruptions. *Transactions of the Society for Design and Process Science* 11(2):91-108.

[Jackson13] Jackson S, Ferris T (2013) Resilience Principles for Engineered Systems. *Systems Engineering* 16(2): 152-164.

[Jajodia11] Jajodia S, Ghosh AK, Swarup V, Wang C, Wang XS (eds.) (2011) *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats* (Springer-Verlag, New York, NY), Advances in Information Security, Vol. 54, pp 184. https://doi.org/10.1007/978-1-4614-0977-9

[Jajodia12] Jajodia S, Ghosh AK, Subrahmanian VS, Swarup V, Wang C, Wang XS (eds.) (2013) *Moving Target Defense II: Application of Game Theory and Adversarial Modeling* (Springer-Verlag, New York, NY), Advances in Information Security, Vol. 100, pp 204.

[JCS17] Joint Chiefs of Staff (2017) Cyber Survivability Endorsement Implementation Guide (CSEIG). (U.S. Department of Defense, Washington, DC), v1.01.

[King12] King S (2012) *National and Defense S&T Strategies & Initiatives*.

[Leveson12] Leveson NG (2012) *Engineering a Safer World: Systems Thinking Applied to Safety* (MIT Press, Cambridge, MA), pp 560.

[Madni07] Madni AM (2007) Designing for Resilience. *ISTI Lecture Notes on Advanced Topics in Systems Engineering* (University of California at Los Angeles (UCLA), Los Angeles, CA).

[Madni09] Madni AM, Jackson S (2009) Towards a Conceptual Framework for Resilience Engineering, *IEEE Systems Journal* 3(2):181-191.

[MITRE07] The MITRE Corporation (2019) *Common Attack Pattern Enumeration and Classification (CAPEC)*. Available at https://capec.mitre.org/index.html

[MITRE18] The MITRE Corporation (2018) *Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)*. Available at https://attack.mitre.org

[MITRE21] The MITRE Corporation (2021) CALDERA™: A Scalable, Automated Adversary Emulation Platform. Available at https://caldera.mitre.org

[Musman18] Musman S, Agbolosu-Amison S, Crowther K (2019) Metrics Based on the Mission Risk Perspective. *Cyber Resilience of Systems and Networks*, eds Kott A, Linkov I (Springer International Publishing, Cham, Switzerland) Chapter 3, pp 41-65. https://doi.org/10.1007/978-3-319-77492-3

[NASA19] National Aeronautics and Space Administration (2019) Systems Engineering Handbook, Section 6.4: Technical Risk Management. Available at https://www.nasa.gov/seh/6-4-technical-risk-management

[Neumann04] Neumann P (2004) Principled Assuredly Trustworthy Composable Architectures. (SRI International, Menlo Park, CA), CDRL A001 Final Report. Available at http://www.csl.sri.com/users/neumann/chats4.pdf

[NIAC10] National Infrastructure Advisory Council (NIAC) (2010) A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations by the Council. (U.S. Department of Homeland Security, Washington, DC). Available at https://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf

[NIST16] National Institute of Standards and Technology Workshop (2016) *Exploring the Dimensions of Trustworthiness: Challenges and Opportunities*. https://www.nist.gov/news-events/events/2016/08/exploring-dimensions-trustworthiness-challenges-and-opportunities

[NIST CSF] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standard, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[ODNI17] Office of the Director of National Intelligence (2017) *Cyber Threat Framework*. Available at https://www.dni.gov/index.php/cyber-threat-framework

[Okhravi13] Okhravi H, Rabe MA, Mayberry TJ, Leonard WG, Hobson TR, Bigelow D, Streilein WW (2013) Survey of Cyber Moving Targets. (Lincoln Laboratory, Lexington, MA), Technical Report 1166. Available at http://web.mit.edu/ha22286/www/papers/LLTechRep.pdf

[Pitcher19] Pitcher S (2019) New DoD Approaches on the Cyber Survivability of Weapon Systems [presentation]. Available at https://www.itea.org/wp-content/uploads/2019/03/Pitcher-Steve.pdf

[Pitcher21] Pitcher S, Andress T (2021) Cyber Survivability for Future and Legacy DoD Weapon Systems [presentation].

[Reilly19] Reilly J (2019) *Cyber Survivability Attributes: CSA Tool (8ABW-2019-2267)* (Air Force Research Laboratory, Rome, NY).

[Ricci14] Ricci N, Rhodes DH, Ross AM (2014) Evolvability-Related Options in Military Systems of Systems. *Procedia Computer Science* 28:314-321. https://doi.org/10.1016/j.procs.2014.03.039

[Richards08] Richards MG, Ross AM, Hastings DE, Rhodes DH (2008) Empirical Validation of Design Principles for Survivable System Architecture. *Proceedings of the 2nd Annual IEEE Systems Conference*, (IEEE, Montreal, Quebec, Canada), pp 1-8. https://doi.org/10.1109/SYSTEMS.2008.4518999

[Richards09] Richards MG, Hastings DE, Rhodes DH, Ross AM, Weigel AL (2009) Design for Survivability: Concept Generation and Evaluation in Dynamic Tradespace Exploration. *Second International Symposium on Engineering Systems* (Massachusetts Institute of Technology, Cambridge, MA). Available at https://pdfs.semanticscholar.org/3734/7b58123c16e84e2f51a4e172ddee0a8755c0.pdf

[SEBoB] BKCASE Editorial Board (2019) The Guide to the Systems Engineering Body of Knowledge (SEBoK), v. 2.0, ed Cloutier RJ (The Trustees of the Stevens Institute of Technology, Hoboken, NJ). BKCASE is managed and maintained by the Stevens Institute of Technology Systems Engineering Research Center, the International Council on Systems Engineering, and the Institute of Electrical and Electronics Engineers Computer Society. Available at http://www.sebokwiki.org/wiki/Guide_to_the_Systems_Engineering_Body_of_Knowledge_(SEBoK)

[Sheard08] Sheard S (2008) A Framework for System Resilience Discussions. *INCOSE International Symposium 18* (Wiley, Utrecht, The Netherlands), pp 1243–1257. https://doi.org/10.1002/j.2334-5837.2008.tb00875.x

[Shetty16] Shetty S, Yuchi X, Song M (2016) *Moving Target Defense for Distributed Systems* (Springer International, Switzerland), pp 76. https://doi.org/10.1007/978-3-319-31032-9

[Sterbenz06] Sterbenz J, Hutchinson D (2006) ResiliNets: Multilevel Resilient and Survivable Networking Initiative. Available at https://www.ittc.ku.edu/resilinets/

[Sterbenz10] Sterbenz JPG, Hutchison D, Çetinkaya EK, Jabbar A, Rohrer JP, Schöller M, Smith P (2010) Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks* 54:1245-1265. Available at http://www.ittc.ku.edu/resilinets/papers/Sterbenz-Hutchison-Cetinkaya-Jabbar-Rohrer-Scholler-Smith-2010.pdf

[Sterbenz14] Sterbenz JP, Hutchison D, Çetinkaya EK, Jabbar A, Rohrer JP, Schöller M, Smith P (2014) Redundancy, diversity, and connectivity to achieve multilevel network resilience, survivability, and disruption tolerance. *Journal of Telecommunications Systems* 56(1):17-31. https://doi.org/10.1007/s11235-013-9816-9

[Strom17] Strom BE, Battaglia JA, Kemmerer MS, Kupersanin W, Miller DP, Wampler C, Whitley SM, Wolf RD (2017) Finding Cyber Threats with ATT&CK-Based Analytics. (The MITRE Corporation, Annapolis Junction, MD), MITRE Technical Report MTR-170202. Available at https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats%20with%20att%26ck-based-analytics.pdf

[Temin10] Temin A, Musman S (2010) A Language for Capturing Cyber Impact Effects. (The MITRE Corporation, Bedford, MA), MITRE Technical Report MTR-100344.

[Zimmerman14] Zimmerman C (2014) Ten Strategies of a World-Class Cybersecurity Operations Center. (The MITRE Corporation, Bedford, MA). Available at http://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf

1717

APPENDIX A

GLOSSARY

COMMON TERMS AND DEFINITIONS

Appendix A provides definitions for terminology used in NIST SP 800-160, Volume 2. Sources for terms used in this publication are cited as applicable. Where no citation is noted, the source of the definition is SP 800-160, Volume 2.

adaptability	The property of an architecture, design, and implementation which can accommodate changes to the threat model, mission or business functions, systems, and technologies without major programmatic impacts.
advanced cyber threat	See *advanced persistent threat*. *Note 1:* The phrase "advanced cyber threat" implies either that an adversary executes a cyber attack or that an adversary subverts the supply chain in order to compromise cyber resources.
advanced persistent threat [SP 800-39]	An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors including, for example, cyber, physical, and deception. These objectives typically include establishing and extending footholds within the IT infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization, or positioning itself to carry out these objectives in the future. The advanced persistent threat pursues its objectives repeatedly over an extended period; adapts to defenders' efforts to resist it; and is determined to maintain the level of interaction needed to execute its objectives. *Note 1:* While some sources define APT (or advanced cyber threat) as an adversary at Tier V or Tier VI in the threat model in [DSB13]—in particular, to be a state actor—the definition used here includes criminal actors. *Note 2:* For brevity, "the APT" refers to any adversary with the characteristics described above or to the set of all such adversaries; "an APT actor" refers to a representative member of that set. *Note 3:* The APT may establish its foothold by subverting the supply chain in order to compromise cyber resources. Thus, the APT may be able to achieve its objectives without executing a cyber attack against the organization's systems (e.g., by inserting a logic bomb or time). *Note 4:* The term "APT" does not include the insider threat. However, if an APT actor establishes and extends its foothold by masquerading as a legitimate system user and taking advantage of that user's authorized access privileges, it may be indistinguishable from an insider threat.

adversity	Adverse conditions, stresses, attacks, or compromises. *Note 1:* The definition of adversity is consistent with the use of the term in [SP 800-160 v1] as disruptions, hazards, and threats. *Note 2:* Adversity in the context of the definition of cyber resiliency specifically includes but is not limited to cyber attacks.
agility	The property of a system or an infrastructure which can be reconfigured, in which resources can be reallocated, and in which components can be reused or repurposed so that cyber defenders can define, select, and tailor cyber courses of action for a broad range of disruptions or malicious cyber activities.
approach	See *cyber resiliency implementation approach*.
asset [SP 800-160 v1]	An item of value to stakeholders. An asset may be tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology component) or intangible (e.g., humans, data, information, software, capability, function, service, trademark, copyright, patent, intellectual property, image, or reputation). The value of an asset is determined by stakeholders in consideration of loss concerns across the entire system life cycle. Such concerns include but are not limited to business or mission concerns.
attack surface [SP 800-53, adapted]	The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from. *Note*: An attack surface can be *reduced* by removing points on the boundary (reducing the *extent* of the attack surface, e.g., by reducing the amount of code running) or reducing the *exposure* of some points to an attacker (e.g., by placing inessential functions on a different system element than essential functions, by layering defenses, by reducing the period of exposure); *changed* by changing the set of points on the boundary (e.g., by moving some points), by changing the exposure of some points to an attacker (e.g., by adding logic to check data or commands), or by changing the properties of some points (e.g., by applying principles of least privilege and least functionality); or *disrupted* by making changes unpredictably or by reducing its extent or exposure for limited time periods (e.g., by temporarily isolating components).
blockchain [IR 8202] [IR 8301]	A distributed digital ledger of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules.
contested cyber environment	An environment in which APT actors, competing entities, and entities with similar resource needs contend for control or use of cyber resources.

control [ISACA]	The means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of an administrative, technical, management, or legal nature. *Note:* See *security control*.
criticality [SP 800-160 v1]	An attribute assigned to an asset that reflects its relative importance or necessity in achieving or contributing to the achievement of stated goals.
cyber incident [CNSSI 4009]	Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein.
cyber resiliency	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. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment. *Note:* Cyber resiliency can be a property of a system, network, service, system-of-systems, mission or business function, organization, critical infrastructure sector or sub-sector, region, or nation.
cyber resiliency concept	A concept related to the problem domain and/or solution set for cyber resiliency. Cyber resiliency concepts are represented in cyber resiliency risk models as well as by cyber resiliency constructs.
cyber resiliency construct	Element of the cyber resiliency engineering framework (i.e., a goal, objective, technique, implementation approach, or design principle). Additional constructs (e.g., sub-objectives or methods, capabilities or activities) may be used in some modeling and analytic practices.
cyber resiliency control	A control (i.e., a base control or a control enhancement) as defined in [SP 800-53], which applies one or more cyber resiliency techniques or approaches or which is intended to achieve one or more cyber resiliency objectives.
cyber resiliency design principle	A guideline for how to select and apply cyber resiliency analysis methods, techniques, approaches, and solutions when making architectural or design decisions.
cyber resiliency engineering practice	A method, process, modeling technique, or analytical technique used to identify and analyze cyber resiliency solutions.
cyber resiliency goal	A high-level statement supporting (or focusing on) one aspect (i.e., anticipate, withstand, recover, adapt) in the definition of cyber resiliency.
cyber resiliency implementation approach	A subset of the technologies and processes of a cyber resiliency technique defined by how the capabilities are implemented or how the intended consequences are achieved.

cyber resiliency objective	A statement of what must be performed (e.g., what a system must achieve in its operational environment and throughout its life cycle) to meet stakeholder needs for mission assurance and resilient security.
cyber resiliency risk model	A risk model which explicitly represents the threats and classes of harm considered by those concerned with cyber resiliency. (This accommodates other stakeholders in addition to systems security engineers.) *Note:* A cyber resiliency risk model emphasizes (but is not limited to) the APT as a threat source and emphasizes the effects of malicious cyber activities on missions, organizations, and systems that include cyber resources.
cyber resiliency solution	A combination of technologies, architectural decisions, systems engineering processes, and operational processes, procedures, or practices that solves a problem in the cyber resiliency domain. A cyber resiliency solution provides enough cyber resiliency to meet stakeholder needs and to reduce risks to mission or business capabilities in the presence of advanced persistent threats.
cyber resiliency sub-objective	A statement, subsidiary to a cyber resiliency objective, which emphasizes different aspects of that objective or identifies methods to achieve that objective.
cyber resiliency technique	A set or class of technologies and processes intended to achieve one or more objectives by providing capabilities to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources. The definition or statement of a technique describes the capabilities it provides and/or the intended consequences of using the technologies or processes it includes.
cyber resource	An information resource which creates, stores, processes, manages, transmits, or disposes of information in electronic form and which can be accessed via a network or using networking methods. *Note:* A cyber resource is an element of a system that exists in or intermittently includes a presence in cyberspace.
cyber risk	The risk of depending on cyber resources (i.e., the risk of depending on a system or system elements which exist in or intermittently have a presence in cyberspace). *Note:* Cyber risk overlaps with security risk [SP 800-160 v1], information security risk [SP 800-30] [CNSSI 4009], cybersecurity risk [IR 8286], and includes risks due to cyber incidents, cybersecurity events, and cyberspace attacks.

cybersecurity [NIST CSF]	The process of protecting information by preventing, detecting, and responding to attacks.
[CNSSI 4009]	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
cybersecurity event [NIST CSF]	A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).
cyberspace [CNSSI 4009] [HSPD23]	The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.
cyberspace attack [CNSSI 4009]	Cyberspace actions that create various direct denial effects (i.e. degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains.
cyber survivability [Pitcher21]	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 its life cycle.
damage	Harm caused to something in such a way as to reduce or destroy its value, usefulness, or normal function. *Note 1:* From the perspective of cyber resiliency, damage can be to the organization (e.g., loss of reputation, increased existential risk), organizational missions or business functions (e.g., decrease in the ability to complete the current mission and to accomplish future missions), security (e.g., decrease in the ability to achieve the security objectives of confidentiality, integrity, and availability or to prevent, detect, and respond to cyber incidents), the system (e.g., decrease in the ability to meet system requirements, unauthorized use of system resources); or specific system elements (e.g., physical destruction; corruption, modification, or fabrication of information). *Note 2*: Damage includes, and in some circumstances can be identified with, asset loss as discussed in [SP 800-160 v1].
design principle	A distillation of experience designing, implementing, integrating, and upgrading systems that systems engineers and architects can use to guide design decisions and analysis. A design principle typically takes the form of a terse statement or a phrase identifying a key concept, accompanied by one or more statements that describe how that concept applies to system design (where "system" is construed broadly to include operational processes and procedures, and may also include development and maintenance environments).

enabling system [ISO 15288]	A system that provides support to the life cycle activities associated with the system-of-interest. Enabling systems are not necessarily delivered with the system-of-interest and do not necessarily exist in the operational environment of the system-of-interest.
enterprise information technology [IEEE17]	The application of computers and telecommunications equipment to store, retrieve, transmit, and manipulate data, in the context of a business or other enterprise.
fault tolerant [SP 800-82]	Of a system, having the built-in capability to provide continued, correct execution of its assigned function in the presence of a hardware and/or software fault.
federation [SP 800-95]	A collection of realms (domains) that have established trust among themselves. The level of trust may vary, but typically includes authentication and may include authorization.
information resources [OMB A-130]	Information and related resources, such as personnel, equipment, funds, and information technology.
information security [OMB A-130]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
information system [OMB A-130]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. *Note:* Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

information technology [OMB A-130]	Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. Information technology does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use.
mission assurance [DOD16, adapted]	A process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to the execution of organizational mission-essential functions in any operating environment or condition. *Note:* This definition differs from the DoD definition by replacing "DoD" with "organizational."
mission resilience [FMRS20, adapted]	The ability to continuously maintain the capability and capacity to perform essential functions and services, without time delay, regardless of threats or conditions, and with the understanding that adequate warning of a threat may not be available. *Note:* This definition differs from the source definition by omitting "of the Federal executive branch" after "the ability." Because essential functions and services are performed using systems, mission resilience can often be identified with operational resilience; usage depends on the intended emphasis.
mitigation	A decision, action, or practice intended to reduce the level of risk associated with one or more threat events, threat scenarios, or vulnerabilities.
non-adversarial threat	A threat associated with accident or human error, structural failure, or environmental causes. *Note:* See [SP 800-30].

operational resilience [CNSSI 4009]	The ability of systems to resist, absorb, and recover from, or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of the ability to perform mission-related functions.
operational technology	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.
other system [ISO 15288]	A system that the system-of-interest interacts with in the operational environment. These systems may provide services to the system-of-interest (i.e., the system-of-interest is dependent on the other systems) or be the beneficiaries of services provided by the system-of-interest (i.e., other systems are dependent on the system-of-interest).
protection [SP 800-160 v1]	In the context of systems security engineering, a control objective that applies across all types of asset types and the corresponding consequences of loss. A system protection capability is a system control objective and a system design problem. The solution to the problem is optimized through a balanced proactive strategy and a reactive strategy that is not limited to *prevention*. The strategy also encompasses avoiding asset loss and consequences; detecting asset loss and consequences; minimizing (i.e., limiting, containing, restricting) asset loss and consequences; responding to asset loss and consequences; recovering from asset loss and consequences; and forecasting or predicting asset loss and consequences.
quality property [SP 800-160 v1]	An emergent property of a system that includes, for example: safety, security, maintainability, resilience, reliability, availability, agility, and survivability. This property is also referred to as a *systemic property* across many engineering domains.
reliability [IEEE90]	The ability of a system or component to function under stated conditions for a specified period of time.
resilience [OMB A-130]	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.
[INCOSE14]	The ability to maintain required capability in the face of adversity.

resilient otherwise [SP 800-160 v1]	Security considerations applied to enable system operation despite disruption while not maintaining a secure mode, state, or transition; or only being able to provide for partial security within a given system mode, state, or transition. See *securely resilient*.
risk [CNSSI 4009] [OMB A-130]	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of the adverse impacts that would arise if the circumstance or event occurs; and the likelihood of occurrence.
risk analysis [ISO 73]	Process to comprehend the nature of risk and to determine the level of risk.
risk assessment [SP 800-39, adapted]	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.
[ISO 73]	Overall process of risk identification, risk analysis, and risk evaluation.
risk-adaptive access control [SP 800-95]	Access privileges are granted based on a combination of a user's identity, mission need, and the level of security risk that exists between the system being accessed and a user. RAdAC will use security metrics, such as the strength of the authentication method, the level of assurance of the session connection between the system and a user, and the physical location of a user, to make its risk determination.
risk factor [SP 800-30]	A characteristic used in a risk model as an input to determining the level of risk in a risk assessment.
risk framing [SP 800-39]	Risk framing is the set of assumptions, constraints, risk tolerances, and priorities/trade-offs that shape an organization's approach for managing risk.
risk management strategy [SP 800-39]	Strategy that addresses how organizations intend to assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions.
risk model [SP 800-30]	A key component of a risk assessment methodology (in addition to assessment approach and analysis approach) that defines key terms and assessable risk factors.
risk response [SP 800-39]	Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.

safety [SP 800-82] [MIL-STD-882E]	Freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.
securely resilient [SP 800-160 v1]	The ability of a system to preserve a secure state despite disruption, to include the system transitions between normal and degraded modes. Securely resilient is a primary objective of systems security engineering.
security [SP 800-160 v1]	Freedom from those conditions that can cause loss of assets with unacceptable consequences.
[ISO 15288]	Protection against intentional subversion or forced failure. A composite of four attributes – confidentiality, integrity, availability, and accountability – plus aspects of a fifth, usability, all of which have the related issue of their assurance.
[CNSSI 4009] [SP 800-37]	A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach. *Note:* See also information security and cybersecurity.
security control [SP 800-160 v1]	A mechanism designed to address needs as specified by a set of security requirements.
security controls [OMB A-130]	The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.
security criteria	Criteria related to a supplier's ability to conform to security-relevant laws, directives, regulations, policies, or business processes; a supplier's ability to deliver the requested product or service in satisfaction of the stated security requirements and in conformance with secure business practices; the ability of a mechanism, system element, or system to meet its security requirements; whether movement from one life cycle stage or process to another (e.g., to accept a baseline into configuration management, to accept delivery of a product or service) is acceptable in terms of security policy; how a delivered product or service is handled, distributed, and accepted; how to perform security verification and validation; or how to store system elements securely in disposal.
security function [SP 800-160 v1]	The capability provided by the system or a system element. The capability may be expressed generally as a concept or specified precisely in requirements.

security relevance [SP 800-160 v1]	The term used to describe those functions or mechanisms that are relied upon, directly or indirectly, to enforce a security policy that governs confidentiality, integrity, and availability protections.
security requirement [SP 800-160 v1]	A requirement that specifies the functional, assurance, and strength characteristics for a mechanism, system, or system element.
survivability [Richards09]	The ability of a system to minimize the impact of a finite-duration disturbance on value delivery (i.e., stakeholder benefit at cost), achieved through the reduction of the likelihood or magnitude of a disturbance; the satisfaction of a minimally acceptable level of value delivery during and after a disturbance; and/or a timely recovery.
system [ISO 15288] [SP 800-160 v1]	Combination of interacting elements organized to achieve one or more stated purposes. *Note 1:* There are many types of systems. Examples include: general and special-purpose information systems; command, control, and communication systems; crypto modules; central processing unit and graphics processor boards; industrial/process control systems; flight control systems; weapons, targeting, and fire control systems; medical devices and treatment systems; financial, banking, and merchandising transaction systems; and social networking systems. *Note 2:* The interacting elements in the definition of system include hardware, software, data, humans, processes, facilities, materials, and naturally occurring physical entities. *Note 3:* System-of-systems is included in the definition of system.
system component [SP 800-53]	Discrete identifiable information technology assets that represent a building block of a system and include hardware, software, firmware, and virtual machines.
system element [ISO 15288] [SP 800-160 v1]	Member of a set of elements that constitute a system. *Note 1:* A system element can be a discrete component, product, service, subsystem, system, infrastructure, or enterprise. *Note 2:* Each element of the system is implemented to fulfill specified requirements. *Note 3:* The recursive nature of the term allows the term *system* to apply equally when referring to a discrete component or to a large, complex, geographically distributed system-of-systems. *Note 4:* System elements are implemented by: hardware, software, and firmware that perform operations on data / information; physical structures, devices, and components in the environment of operation; and the people, processes, and procedures for operating, sustaining, and supporting the system elements.

system-of-interest [SP 800-160 v1]	A system whose life cycle is under consideration in the context of [ISO/IEC/IEEE 15288:2015]. *Note:* A system-of-interest can be viewed as the system that is the focus of the systems engineering effort. The system-of-interest contains system elements, system element interconnections, and the environment in which they are placed.
system-of-systems [SP 800-160 v1] [INCOSE14]	System-of-interest whose system elements are themselves systems; typically, these entail large-scale interdisciplinary problems with multiple heterogeneous distributed systems. *Note:* In the system-of-systems environment, constituent systems may not have a single owner, may not be under a single authority, or may not operate within a single set of priorities.
technical risk [NASA19]	The risk associated with the evolution of the design and the production of the system of interest affecting the level of performance necessary to meet the stakeholder expectations and technical requirements. *Note*: Technical risk is often associated with novel technologies being proposed for integration into the system-of-interest or being used in systems which interact with the system-of-interest. It can also be associated with new discoveries of inherent vulnerabilities in technologies, or with products being withdrawn from use or losing support.
technique	See *cyber resiliency technique*.
threat event [SP 800-30]	An event or situation that has the potential for causing undesirable consequences or impact.
threat scenario [SP 800-30]	A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time.
threat source [CNSSI 4009]	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.
trustworthiness [SP 800-160 v1]	Worthy of being trusted to fulfill whatever critical requirements may be needed for a particular component, subsystem, system, network, application, mission, business function, enterprise, or other entity.
zero trust architecture [EO 14028]	A security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The zero trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses.

1724

1725 APPENDIX B

1726 # ACRONYMS

1727 COMMON ABBREVIATIONS

ABAC	Attribute-Based Access Control
AFRL	Air Force Research Laboratory
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
ASIC	Application-Specific Integrated Circuit
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge
BIA	Business Impact Analysis
BMS	Building Management Systems (BMS)
C3	Command, Control, and Communications
CAN	Controller Area Network
CAPEC	Common Attack Pattern Enumeration and Classification
CCoA	Cyber Courses of Action
CDM	Continuous Diagnostics and Mitigation
CERT	Computer Emergency Response Team
CIS	Critical Infrastructure System
CJA	Crown Jewels Analysis
CLI	Command Line Interface
CMIA	Cyber Mission Impact Analysis
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COOP	Continuity of Operations *or* Continuity of Operations Plan
COTS	Commercial Off-The-Shelf
CPS	Cyber-Physical System or Systems
CRR	Cyber Resilience Review
CSA	Cyber Survivability Attributes
CSRC	Computer Security Resource Center
CTI	Cyber Threat Intelligence

CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DMZ	Demilitarized Zone
DNS	Domain Name System
DoD	Department of Defense
DSB	Defense Science Board
DSP	Digital Signal Processor
ECU	Embedded Control Unit
E-ISAC	Electricity ISAC
EIT	Enterprise Information Technology
EMS	Energy Management System
ERM	Enterprise Risk Management
FDNA	Functional Dependency Network Analysis
FPGA	Field-Programmable Gate Array
FMECA	Failure Modes, Effects, and Criticality Analysis
FIPS	Federal Information Processing Standard(s)
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
FOSS	Free and Open Source Software
GPS	Global Positioning System
HACS	Highly Adaptive Cybersecurity Services
HDL	Hardware Description Language
HMI	Human-Machine Interface
HVA	High-Value Asset
HVAC	Heating, Ventilation, and Air Conditioning
I&W	Indications and Warnings
IdAM	Identity and Access Management
IACD	Integrated Adaptive Cyber Defense
ICAM	Identity, Credential, and Access Management
ICS	Industrial Control System
ICT	Information and Communications Technology
IDS	Intrusion Detection System

IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INCOSE	International Council on Systems Engineering
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
ITL	Information Technology Laboratory
LSPE	Large-Scale Processing Environment
MCU	Master Control Unit
MFA	Multi-Factor Authentication
MIA	Mission Impact Analysis
MIL-STD	Military Standard
M&S	Modeling and Simulation
MBSE	Model-Based Systems Engineering
ML	Machine Learning
MOE	Measure of Effectiveness
MOP	Measure of Performance
MTD	Moving Target Defense
NASA	National Aeronautics and Space Administration
NDIA	National Defense Industrial Association
NIAC	National Infrastructure Advisory Council
NIST	National Institute of Standards and Technology
NoT	Network of Things
OEM	Original Equipment Manufacturer
OMB	Office of Management and Budget
OPSEC	Operations Security
OT	Operational Technology
PBX	Private Branch Exchange
PETE	Potential Efforts on Threat Events
PII	Personally Identifiable Information
PLC	Programmable Logic Controller
PPD	Presidential Policy Directive
RAdAC	Risk-Adaptive Access Control

RAID	Redundant Array of Independent Disks
RBAC	Role-Based Access Control
RMA	Reliability, Maintainability, Availability
RMF	Risk Management Framework
RMM	Resilience Management Model
ROI	Return on Investment
RTU	Remote Terminal Unit
RSWG	(INCOSE) Resilient Systems Working Group
SAE	Society of Automotive Engineers
SCADA	Supervisory Control and Data Acquisition
SCRM	Supply Chain Risk Management
SDN	Software Defined Networking
SEI	Software Engineering Institute
SME	Subject Matter Expert
SOC	Security Operations Center
SOW	Statement of Work
SP	Special Publication
SSE	Systems Security Engineering
STAMP	Systems-Theoretic Accident Model and Processes
STPA	System-Theoretic Process Analysis
TTP	Tactics, Techniques, and Procedures
TTX	Table Top Exercise
UPS	Uninterruptible Power Supply
VCU	Vehicle Control Unit
VOA	Voice of the Adversary
VOIP	Voice over Internet Protocol
VPN	Virtual Private Network
ZT	Zero Trust
ZTA	Zero Trust Architecture

1728

APPENDIX C

BACKGROUND

CYBER RESILIENCY IN CONTEXT

This appendix provides background and contextual information on cyber resiliency. It describes how the definition of cyber resiliency relates to other forms of resilience; the distinguishing characteristics of cyber resiliency, including the assumptions that underpin this specialty engineering discipline; the relationship between cyber resiliency engineering and other specialty engineering disciplines; and the relationship between cyber resiliency and risk.

C.1 DEFINING CYBER RESILIENCY

Cyber resiliency[85] is defined as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources." This definition can be applied to a variety of entities 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;[86]
- A critical infrastructure sector or a region;
- A system-of-systems in a critical infrastructure sector or sub-sector; and
- The Nation.

Cyber resiliency is emerging as a key element in any effective strategy for mission assurance, business assurance, or operational resilience. The definition of cyber resiliency is informed by definitions of the terms *resilience* and *resiliency* across various communities of interest, as illustrated in the following examples (*italics* added to highlight common goals):

[85] "Resilience" and "resiliency" are alternative spellings with resilience being more common. The term *cyber resiliency* is used in the cyber resiliency engineering framework described in this publication to avoid creating the impression that cyber resiliency engineering is a sub-discipline of resilience engineering. See Section C.2 for a discussion of the relationship. The term *cyber resilience* is used by many organizations to refer to organizational resilience against cyber threats with a strong emphasis on effective implementation of good cybersecurity practices and COOP. For example, the DHS Cyber Resilience Review (CRR), which is based on the Software Engineering Institute (SEI) CERT Resilience Management Model (RMM), focuses on good practices against conventional adversaries. Discussions of cyber resilience focus on improved risk governance (e.g., making cyber risk part of enterprise risk), improved cyber hygiene to include incident response procedures and ongoing monitoring, and threat information sharing. These aspects of governance and operations are all important to an organization's cyber preparedness strategy [Bodeau16]. However, discussions of cyber resilience in the sense of operational resilience against cyber threats, generally omit the architecture and engineering aspect, which is the focus of the cyber resiliency engineering framework and the design principles discussed in this publication.

[86] See [SP 800-39] for a discussion of the system, mission/business function, and organization levels. See [NIST CSF] for a discussion of critical infrastructure levels. See [SP 800-37, SP 800-160 v1] for a discussion of system-of-systems.

- **Resilience for the Nation:** The ability to *adapt* to changing conditions and *withstand* and rapidly *recover* from emergencies [PPD8].
- **Critical Infrastructure Resilience:** The ability to reduce the magnitude or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to *anticipate, absorb, adapt* to, and/or rapidly *recover* from a potentially disruptive event [NIAC10].
- **Resilience for National Security Systems:** The ability to *prepare* for and *adapt* to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to *withstand* and *recover* from deliberate attacks, accidents, or naturally occurring threats or incidents [CNSSI 1253] [SP 800-37].
- **Community Resilience:** The ability of a community to *prepare* for anticipated hazards, *adapt* to changing conditions, *withstand* and *recover* rapidly from disruptions [SP 1190].
- **Critical Infrastructure Security and Resilience:** The ability to *prepare* for and *adapt* to changing conditions and *withstand* and *recover* rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents [PPD21].
- **Information System Resilience:** The ability of a system to *continue* to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities and *recover* to an effective operational posture in a time frame consistent with mission needs [SP 800-53].
- **Resilience in Cyberspace:** The ability to *adapt* to changing conditions and *prepare* for, *withstand*, and rapidly *recover* from disruption [DHS10].
- **Network Resilience:** The ability of the network to provide and *maintain* an acceptable level of service in the face of various faults and challenges to normal operation [Sterbenz06].
- **Operational Resilience:** The ability of systems to *resist, absorb*, and *recover* from or *adapt* to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions [CNSS 4009].
- **Resilience Engineering:** The ability to build systems that can *anticipate* and circumvent accidents, *survive* disruptions through appropriate learning and *adaptation*, and *recover* from disruptions by restoring the pre-disruption state as closely as possible [Madni09].

Despite the different scope covered by each definition, there are some commonalities across the definitions. Each definition expresses a common theme of addressing those situations or conditions in which disruption, adversity, errors, faults, or failures occur. The definitions express consistent resiliency goals (shown in *italics* above) when encountering specific situations or conditions causing disruption, adversity, and faults. The definition of cyber resiliency adopted for use in this publication is consistent with the definitions cited above.

C.2 DISTINGUISHING CHARACTERISTICS OF CYBER RESILIENCY

Any discussion of cyber resiliency is distinguished by its focus and *a priori* threat assumptions. These are reflected in cyber resiliency constructs and engineering practices.

- **Focus on the mission or business functions.**

  Discussions of cyber resiliency focus on capabilities supporting organizational missions or business functions in order to maximize the ability of organizations to complete critical or essential missions or business functions despite an adversarial presence in their systems and infrastructure threatening mission-critical systems and system components. This is in contrast to focusing on the protection of information or on ensuring capabilities in a non-adversarial environment. It is also in contrast to focusing on ensuring the resilience of system elements or of constituent systems in a system-of-systems. From the perspective of cyber resiliency, system elements or constituent systems that are less critical to mission or business effectiveness can be sacrificed to contain a cyber attack and maximize mission assurance.

- **Assume a changing environment.**

  Discussions related to cyber resiliency assume ongoing and episodic changes in the threat environment, the operational environment, and the technical environment. APT actors learn from experience. Their motives can change in response to economic and political factors, and their TTPs can become commodity tools for lower-level actors. The ways technology is used by individuals and organizations change due to events such as the COVID-19 pandemic, broader or more cost-effective availability of services such as cloud computing, and growing familiarity with and acceptance of newer technologies. The technical environment continues to evolve, such as with the rapid convergence of information technology and operational technology, the increasing maturity of artificial intelligence and machine learning, and the transition to zero trust architectures. These changes can interact in many ways, increasing the complexity and reducing the transparency of systems, services, infrastructures, and ecosystems. From the perspective of cyber resiliency, changes can simultaneously present risks and opportunities for risk reduction. Risk management needs to consider differences in scale and time frame.

- **Focus on the effects of the advanced persistent threat.**

  The definition of cyber resiliency encompasses all threats to systems containing cyber resources, whether such threats are cyber or non-cyber (e.g., kinetic) in nature. However, cyber resiliency analysis focuses on the effects that the APT can have on the system-of-interest and, thereby, on the missions or business functions, organization, or external stakeholders.

  In addition to immediately detectable effects (e.g., destruction of data, malfunction of a CPS, denial of service), the APT can produce effects that are detectable only after extended observation or forensic analysis of the system-of-interest (e.g., escalation of privileges, modification or fabrication of data or services, exfiltration of data). Consideration of cyber resiliency in systems security engineering seeks to mitigate such effects, independent of when or whether they may be detected.

  The resources associated with the APT, its stealthy nature, its persistent focus on the target of interest, and its ability to adapt in the face of defender actions make it a highly dangerous threat. Moreover, the APT can take advantage of or make its behavior appear to result from other forms of adversity, including human error, structural failure, or natural disaster. By focusing on APT activities and their potential effects, systems engineers produce systems that can anticipate, withstand, recover from, and adapt to a broad and diverse suite of adverse conditions and stresses on systems containing cyber resources.

- **Assume the adversary will compromise or breach the system or organization.**

  A fundamental assumption in any discussion of cyber resiliency is that a sophisticated adversary cannot always be kept out of a system or be quickly detected and removed from that system, despite the quality of the system design, the functional effectiveness of the security components, and the trustworthiness of the selected components. This assumption acknowledges that modern systems are large and complex entities, and adversaries will always be able to find and exploit weaknesses and flaws in the systems (e.g., unpatched vulnerabilities, misconfigurations), environments of operation (e.g., social engineering, user vulnerability), and supply chains. As a result, a sophisticated adversary can penetrate an organizational system and achieve a presence within the organization's infrastructure.

- **Assume the adversary will maintain a presence in the system or organization.**

  Any discussion of cyber resiliency assumes that the adversary presence may be a persistent and long-term issue and recognizes that the stealthy nature of the APT makes it difficult for an organization to be certain that the threat has been eradicated. It also recognizes that the ability of the APT to adapt implies that previously successful mitigations may no longer be effective. Finally, it recognizes that the persistent nature of the APT means that even if an organization has succeeded in eradicating its presence, it may return. In some situations, the best outcome that an organization can achieve is containing the adversary's malicious code or slowing its lateral movement across the system (or transitively across multiple systems) long enough that the organization is able to achieve its primary mission prior to losing its critical or essential mission capability.

C.3 RELATIONSHIP WITH OTHER SPECIALITY ENGINEERING DISCIPLINES

Cyber resiliency is an aspect of trustworthiness, as are safety, system resilience, survivability, reliability, and security.[87] Cyber resiliency concepts and engineering practices assume a basic foundation of security and reliability. Many cyber resiliency techniques use or rely on security, reliability, resilience, and fault-tolerance mechanisms, and many cyber resiliency techniques and design principles are relevant to zero trust architectures. The concepts and engineering practices described in this publication build on work in the specialty engineering disciplines of resilience engineering and dependable computing, including survivability engineering and fault tolerance.

- **Safety**

  Safety is defined as "freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment" [SP 800-82]. Safety engineering focuses on identifying unacceptable system behaviors, outcomes, and interactions and helping to ensure that the system does not enter an unacceptable state (i.e., a state in which such behaviors, interactions, or outcomes are possible, thus creating or being an instance of a condition that can cause one of the harms identified above). System safety engineering is based on analytic processes rather than design principles or constructs.

[87] Trustworthiness requirements can include attributes of reliability, dependability, performance, resilience, safety, security, and survivability under a range of potential adversity in the form of disruptions, hazards, and threats [SP 800-53].

[SP 800-160 v1] states that "the system aspects of secure operation may intersect, complement, or be in direct conflict or contradiction with those of safe operation of the system." A similar statement may be made with respect to cyber-resilient operations. The set of unacceptable states defined by safety engineering may constitute a constraint on cyber resiliency solutions or may be used in trade-off analyses. As part of achieving a specific cyber resiliency objective, such as Continue or Reconstitute,[88] a system may need to operate transiently in an unsafe (or insecure) state, depending on how stakeholders prioritize and trade off required system properties and behaviors.

- **Security**

The relationship between cyber resiliency and security depends on which definition of security is considered. [SP 800-37] defines security as:

> "A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach."

This definition of security overlaps with but does not subsume cyber resiliency since "protective measures," as listed in the definition, do not fully cover risk management strategies related to cyber resiliency.[89]

Cyber resiliency engineering may be viewed as a specialty discipline of systems security engineering. [SP 800-160 v1] defines security as the "freedom from those conditions that can cause loss of assets with unacceptable consequences."[90] In that context, security is concerned with the protection of assets and is primarily oriented to the concept of asset loss.[91] It includes but is not limited to cybersecurity.[92] Cyber resiliency engineering is oriented toward capabilities and harms to systems containing cyber resources. This orientation is consistent with the concept of asset loss since a capability is a form of intangible asset. As noted above, cyber resiliency engineering focuses on capabilities that support missions or business functions and on the effects of adversarial actions on systems.

[88] See Section 2.1.2.

[89] See Section C.4.

[90] This is a broader construction than what appears in [FIPS 199]. In accordance with [FISMA], FIPS 199 defines three security objectives for information and information systems: confidentiality, integrity, and availability. A loss of confidentiality is the unauthorized disclosure of information; a loss of integrity is the unauthorized modification or destruction of information; and a loss of availability is the disruption of access to or use of information or an information system.

[91] The term *protection*, in the context of systems security engineering, has a very broad scope and is primarily a control objective that applies across all asset types and corresponding consequences of loss. Therefore, the system protection capability is a system control objective and a system design problem. The solution to the problem is optimized through a balanced proactive and reactive strategy that is not limited to prevention. The strategy includes avoiding, detecting, minimizing (i.e., limiting, containing, restricting), responding to, recovering from, and forecasting or predicting asset loss and consequences [SP 800-160 v1].

[92] Cybersecurity is defined as "the process of protecting information by preventing, detecting, and responding to attacks" [NIST CSF] or as the "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation" [OMB A-130].

While [SP 800-160 v1] views security, asset loss, and protection broadly, much of the security literature and many security practitioners focus narrowly on the security objectives of confidentiality, integrity, and availability of information and information systems [FIPS 199].[93] Cyber resiliency engineering considers a broader range of cyber effects (i.e., effects in cyberspace) than the loss of confidentiality, integrity, or availability of information or of system services. Cyber effects of concern to cyber resiliency engineering do include the effects of concern to security, including service degradation and denial or interruption of service; non-disruptive modification, fabrication, corruption, or destruction of information resources; and unauthorized disclosure of information. In addition, they include the usurpation or unauthorized use of resources, even when such use is non-disruptive to the system-of-interest; reduced confidence in system capabilities, which can alter system usage behavior; and alterations in behaviors that affect external systems, which can result in cascading failures beyond the system-of-interest.

As noted above, cyber resiliency concepts and engineering practices assume a foundation of security. Some cyber resiliency techniques[94] rely on the correct and effective application of security controls. Some cyber resiliency design principles[95] adapt or are strongly aligned with the security design principles described in [SP 800-160 v1].

- **Zero Trust**

  Zero trust is a security paradigm for enterprise computing with extensions to other computing environments (e.g., operational technology networks). A zero trust architecture (ZTA) can be characterized as a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside of traditional network boundaries [EO 14028]. Thus, cyber resiliency and zero trust share assumptions about cyber threats. However, where cyber resiliency is motivated by mission assurance in a contested cyber environment, zero trust is focused on preventing unauthorized access to data and services [SP 800-207].

  Cyber resiliency includes a large number of constructs with the assumption that these will be interpreted, prioritized, and down-selected for a given organization, mission or business function, or system-of-interest. Thus, two architectures can be equally cyber-resilient while providing radically different capabilities. By contrast, the expectation for a ZTA is that it will provide comprehensive security monitoring, granular risk-based access controls, and system security automation [EO 14028]. As noted in Section D.4 and Section D.5, multiple cyber resiliency techniques, approaches, and design principles can be integrated into the design and deployment of a ZTA, and some cyber resiliency techniques (e.g., Segmentation, Privilege Restriction) are essential to ZT.

- **Resilience Engineering and Survivability Engineering**

  The specialty disciplines of resilience engineering and survivability engineering address system resilience whether or not the system-of-interest contains cyber resources. Cyber resiliency concepts and engineering practices assume that some of the system elements are cyber resources. Resilience engineering is "the ability to build systems that can anticipate and circumvent accidents, survive disruptions through appropriate learning and adaptation,

[93] Note that [SP 800-160 v1] adapts these security objectives to be more broadly applicable.

[94] See Section 2.1.3.

[95] See Section 2.1.4.

and recover from disruptions by restoring the pre-disruption state as closely as possible" [Madni07, Madni09]. Survivability engineering can be viewed as the subset of systems engineering concerned with minimizing the impact of environmental disturbances on system performance. Survivability is defined as:

> …the ability of a system to minimize the impact of a finite-duration disturbance on value delivery (i.e., stakeholder benefit at cost), achieved through the reduction of the likelihood or magnitude of a disturbance; the satisfaction of a minimally acceptable level of value delivery during and after a disturbance; and/or a timely recovery [Richards09].

Cyber resiliency engineering draws upon concepts and design principles from resilience engineering and survivability engineering. However, as discussed further in Section D.4, the threat model for cyber resiliency differs from the model typically used in these specialty engineering disciplines, which assume detectable disruptions. The concepts and design principles for survivability and resilience are adapted or extended to reflect malicious cyber activities that can remain undetected for extended periods.

- **Cyber Survivability**

  Cyber survivability is defined in [Pitcher19], [Pitcher21], and [JCS17] 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 its life cycle." Cyber survivability is defined for warfighter systems (e.g., weapons systems, supporting critical infrastructures), and in that context, is conceptually identical to cyber resiliency.

  Engineering for cyber survivability focuses on defining and evaluating Cyber Survivability Attributes (CSAs), which are system capabilities that support and serve as indicators of cyber survivability. The CSAs align with the cyber resiliency goals: CSA01-06 with Anticipate, CSA07-08 with Withstand, CSA09 with Recover, and CSA10 with Adapt. Many CSAs depend on the same security measures and other functionality as cyber resiliency techniques and implementation approaches (e.g., performance monitoring; identity, credential, and access management; and logging and auditing). Systems engineers can employ cyber resiliency techniques in the design and implementation of a system to provide the CSA-required functionality or to make that functionality more effective against threat actions.[96]

- **Reliability**

  Reliability is defined as "the ability of a system or component to function under stated conditions for a specified period of time" [IEEE90]. Reliability engineering shares many analytic techniques with safety engineering but focuses on failures of systems or system components rather than on potential harms. Cyber resiliency engineering assumes that reliability, including the consideration of degradation and failure, is addressed in the overall systems engineering process. The threat model, including the stated conditions for reliability, typically does not include deliberate adversarial behavior and necessarily excludes new and unanticipated attack methods developed by advanced adversaries.

[96] The CSA tool created by the Air Force Research Laboratory (AFRL) [Reilly19] captures relationships between controls and control enhancements in [SP 800-53], which support cyber resiliency (see Table E.1) and the CSAs. The CSA tool also captures the mappings of cyber resiliency controls and implementation approaches to ATT&CK techniques (see Appendix F).

- **Fault Tolerance**

  A fault-tolerant system is one with "the built-in capability to provide continued, correct execution of its assigned function in the presence of a hardware and/or software fault" [SP 800-82]. Classes of faults include development faults, physical faults, and interaction faults. Faults can be characterized by the phase of creation or occurrence whether they are internal or external to a system, natural or human-made, or in hardware, software, persistence, and properties related to human-made faults [Avizienis04]. An advanced adversary can cause, emulate, or take advantage of a fault. Cyber resiliency engineering draws some techniques or approaches[97] from fault tolerance and leverages these capabilities while assuming that the actions of an advanced adversary may go undetected.

The analytic processes and practices related to cyber resiliency are intended to be integrated with those for other specialty engineering disciplines, including security, systems engineering, resilience engineering, safety, cybersecurity, and mission assurance. Examples of analytic practices from these disciplines include:

- **Security, Information Security, and Cybersecurity:** Operations security (OPSEC) analysis (see SC-38 in [SP 800-53]), information security risk analysis [SP 800-30], coverage analysis with respect to a taxonomy of attack events or TTPs [DHSCDM], attack tree or attack graph analysis, attack surface analysis, adversary emulation [MITRE21], and Red Team or penetration testing analysis
- **Resilience Engineering:** Criticality Analysis [IR 8179], Mission Impact Analysis (MIA), Business Impact Analysis (BIA) [SP 800-34], fault tree analysis, and Failure Modes, Effects, and Criticality Analysis (FMECA)
- **Systems Engineering:** Modeling and simulation (M&S), model-based systems engineering (MBSE), and Functional Dependency Network Analysis (FDNA)
- **Safety:** Fault tree analysis, FMECA, System-Theoretic Process Analysis (STPA), and Systems-Theoretic Accident Model and Processes (STAMP) [Leveson12]
- **Mission Assurance:** Crown Jewels Analysis (CJA), mission thread analysis, cyber mission impact analysis (CMIA), and supply chain risk management (SCRM) analysis [SP 800-161]

These existing analytic practices are extensible (and in practice have been extended) to include cyber resiliency concepts and concerns, particularly the growing concern that an advanced adversary can establish a covert and persistent presence on a specific system-of-interest, enabling system, or another system in the environment of operation of the system-of-interest. Additional analytic practices include structured analysis of the system architecture and design with respect to cyber resiliency design principles, techniques, and approaches and adaptation of coverage analysis to include effects on adversary activities described in Appendix F.

C.4 RELATIONSHIP BETWEEN CYBER RESILIENCY AND RISK

Cyber resiliency solutions are intended to reduce the risk to missions or business functions, organizations, and individuals that depend on systems containing cyber resources. This cyber risk arises in several ways. For example, cyber resources and the systems that incorporate those

[97] See Section 2.1.3.

resources are increasingly complex, so their behavior and properties in the presence of adversity (or even under expected levels of stress) can be difficult to predict. Software generally includes vulnerabilities and weaknesses, which can make it fragile and subject to exploitation by an adversary. Additionally, the presence of resources in cyberspace exposes them to cyber attacks.[98]

Cyber resiliency solutions are intended to reduce the risk of depending on systems that contain cyber resources by reducing the extent of the harm from threat events,[99] the likelihood of the occurrence of threat events, and the likelihood that threat events will cause harm.[100] The risk model for cyber resiliency identifies the types of threat events and the classes of harm of interest to systems security engineers concerned with cyber resiliency. The extent of potential risk mitigation due to a cyber resiliency solution can be analyzed and assessed in the context of that risk model.

The *risk model* for cyber resiliency builds on risk models for security, cybersecurity, resilience engineering, and survivability. However, the cyber resiliency risk model emphasizes the APT and the effects on missions and organizations of malicious cyber activities or of harm to systems that include cyber resources. Thus, the threat model and the consequence model components of the cyber resiliency threat model have distinctive characteristics.

The *threat model* for cyber resiliency encompasses conventional security threat models that consider threat sources, including accident and human error, structural failure of system elements or supporting infrastructures, natural disasters, and deliberate human actions (including those by malicious insiders). Similarly, the threat model for cyber resiliency encompasses typical cybersecurity risk models.[101] However, the cyber resiliency threat model emphasizes the APT as a primary or secondary threat source. As a primary threat source, sophisticated adversaries execute cyber campaigns that can involve multiple systems and organizations and extend for periods of months or even years.[102] In addition, these adversaries can use TTPs typical of less sophisticated cyber threat actors. As a secondary threat source, the APT can take advantage of threat events due to infrastructure failure or natural disasters and imitate or leverage human error or the loss of component reliability. Therefore, when cyber resiliency engineering analysis considers a potential disruption with a non-adversarial source, that analysis includes looking for ways in which the APT could take advantage of the disruption.

[98] The risk due to the potential for a cyber attack (i.e., an attack via cyberspace, targeting an organization's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure; destroying the integrity of data; or stealing controlled information [SP 800-39]) is also referred to as cybersecurity risk [NIST CSF].

[99] The term *threat event* refers to an event or situation that has the potential for causing undesirable consequences or impacts. Threat events can be caused by either adversarial or non-adversarial threat sources [SP 800-30].

[100] While many different risk models are potentially valid and useful, three elements are common across most models: the likelihood of occurrence, the likelihood of impact, and the level of the impact [SP 800-30].

[101] [EO 13800] states that "cybersecurity risk management comprises the full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of, respond to, and recover from incidents." While the term *cyber threat* is used without definition in such sources as [EO 13800], [ODNI17], [DSB13], and [DHSCDM], its use (without the qualification of "advanced") generally implies that the cyber threat actor attacks via cyberspace.

[102] Activities and threat events can be obtained from [MITRE18] or [SP 800-30] with augmentation or additional detail from other sources. The stages or phases of a cyber attack can be obtained from [MITRE18] or [ODNI17].

The *consequence model* for cyber resiliency encompasses consequences to information and information systems (i.e., a loss of confidentiality, integrity, or availability, as defined in [FIPS 199]). These general consequences can be translated into more specific harms to information and systems that include or are enabled by cyber resources: degraded or disrupted functionality or performance; modified, corrupted, or fabricated information; usurped or misused system resources; or exfiltrated or exposed information. However, the consequence model for cyber resiliency also considers the potential consequences to the missions or business functions supported by the system, to the organization, and sometimes to other stakeholders (e.g., individuals whose personal information may be exfiltrated or exposed, members of the public affected by environmental harms resulting from failure of a critical infrastructure system). In general, a cyber resiliency solution identified and implemented for a given scope is intended to reduce risks at the next level; for example, implementing a solution at the system level can mitigate risks to mission or business function.

Consequences to a mission or business function or to an organization can be defined in terms of impacts on the performance of required functions or on preserving required properties. The risk model for cyber resiliency, therefore, aligns well with mission risk models [Musman18]. It can also be used in conjunction with risk models that represent quality properties, such as security, survivability, and resilience.[103]

- **Security:** The threat model for cyber resiliency encompasses the security threat model but emphasizes the APT. Depending on how broadly (e.g., all stakeholder trustworthiness concerns) or narrowly (e.g., specific stakeholder concerns for confidentiality, integrity, or availability) security is construed, the cyber resiliency consequence model can coincide with or include the security consequence model. The consequence model requires the systems engineers analyzing risks to view the system-of-interest in terms of how its environment of operation[104] imposes constraints and also how adversity involving cyber resources and, consequently, the system-of-interest affect that environment.
- **Resilience engineering and survivability:** The threat model for resilience engineering and survivability focuses on an event or a set of circumstances that disrupts performance. Survivability considers finite-duration events, while resilience engineering also considers multiple or repeated events and changes in the operational environment. In either case, the threat model implicitly assumes that the event or its immediate consequences can be detected. The threat model for cyber resiliency, by contrast, assumes that an advanced adversary can operate covertly in the system for an extended period before causing a detectable disruption. The consequence model is also different. Adversary-caused harms, such as the fabrication of user accounts or the exfiltration of sensitive information, may be non-disruptive. Disruption of normal system performance may, in fact, result from defensive actions taken after such harms are detected (e.g., removing compromised or suspect components from the system). Thus, the consequence model for cyber resiliency encompasses the consequence model for resilience and survivability.

[103] *Quality properties* are emergent properties of systems that may include safety, security, maintainability, resilience, reliability, availability, agility, and survivability [SP 800-160 v1]. These properties are also referred to as *systemic properties* across many engineering domains.

[104] See Figure 2 in [SP 800-160 v1].

APPENDIX D

CYBER RESILIENCY CONSTRUCTS

ENGINEERING FRAMEWORK CONSTRUCTS AND RELATIONSHIPS

This appendix provides an in-depth description of the cyber resiliency constructs that are part of the cyber resiliency engineering framework. The constructs include cyber resiliency goals, objectives, techniques, implementation approaches, strategic design principles, and structural design principles. The appendix also describes the relationships among constructs to assist stakeholders in the application of the contructs.

D.1 CYBER RESILIENCY GOALS

Cyber resiliency, similar to security, is a concern at multiple levels in an organization. The cyber resiliency goals (i.e., anticipate, withstand, recover, and adapt) support the linkage between the risk management decisions at the mission or business process and system levels and the organization's risk management strategy [SP 800-39].

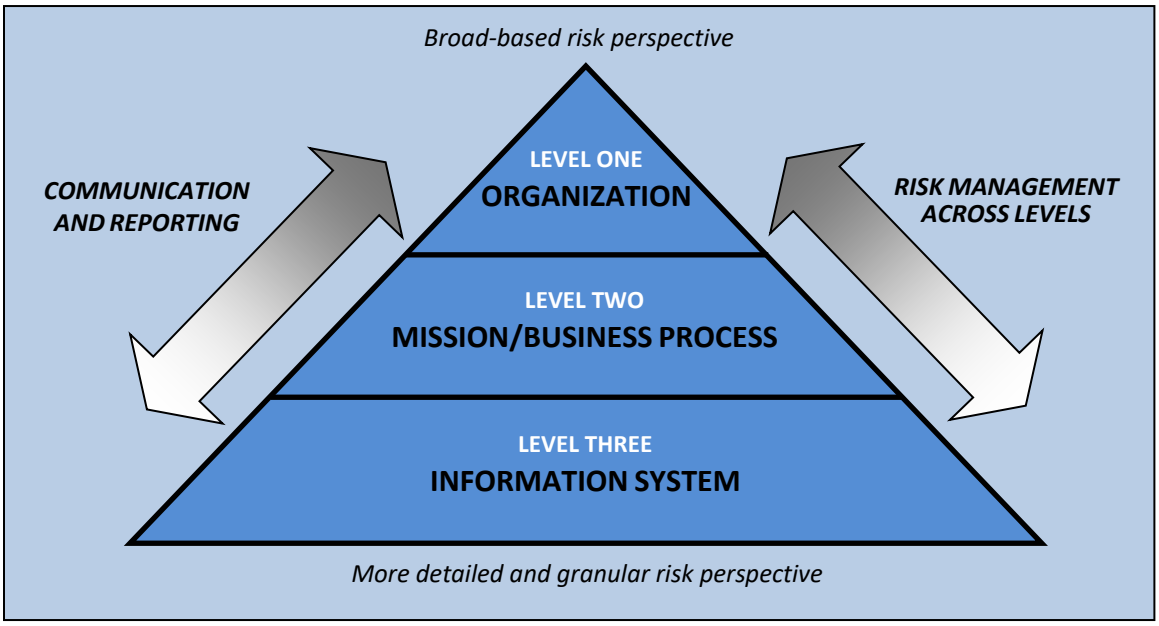

FIGURE D-1: ORGANIZATION-WIDE RISK MANAGEMENT APPROACH

To address cyber resiliency, an organization's risk management strategy needs to include its threat-framing with respect to cyber threats, its strategies for achieving cyber resiliency goals, and its choice of factors to use when prioritizing and interpreting cyber resiliency objectives at the mission or business process level and at the system level. Strategies for achieving cyber resiliency goals include:

- **Anticipate:** Deterrence, avoidance, and prevention are strategies for anticipating potential threats. Other strategies include planning (i.e., identifying available resources and creating plans for using those resources if a threat materializes), preparation (i.e., changing the set of available resources and exercising plans), and morphing (i.e., changing the system on an ongoing basis in order to change the attack surface).

- **Withstand:** Strategies for withstanding the realization of potential threats, even when those threats are not detected, include absorption (i.e., accepting some level of damage to a given set of system elements, taking actions to reduce the impacts to other system elements or to the system as a whole, and repairing damage automatically), deflection (i.e., transferring threat events or their effects to different system elements or to systems other than those that were targeted or initially affected), and discarding (i.e., removing system elements or even a system as a whole based on indications of damage and either replacing those elements or enabling the system or mission or business process to operate without them).
- **Recover:** Strategies for recovery include reversion (i.e., replicating a prior state that is known to be acceptable), reconstitution (i.e., replicating critical and supporting functions to an acceptable level or using existing system resources), and replacement (i.e., replacing damaged, suspect, or selected system elements with new ones or repurposing existing system elements to serve different functions in order to perform critical and supporting functions, possibly in different ways). Detection can support the selection of a recovery strategy. However, a system can apply these strategies independent of detection to change the attack surface.
- **Adapt:** Strategies for adaptation include correction (i.e., removing or applying new controls to compensate for identified vulnerabilities or weaknesses), hardening (i.e., reducing or manipulating attack surfaces), and reorientation (i.e., proactively orienting controls, practices, and capabilities to prospective, emerging, or potential threats). These strategies may result in redefinition (i.e., changing the system's requirements, architecture, design, configuration, acquisition processes, or operational processes).

The organizational risk management strategy includes aspects that can limit the set of cyber resiliency solutions it will consider. These aspects include:[105]

- The organization's risk mitigation philosophy (e.g., compliance with standards of good practice, incorporating state-of-the-art technologies and making trade-offs between standards of good practice and leading-edge protection technologies, pushing the state-of-the-art through cyber defense DevOps)
- Dependencies and interactions among the organization's programs, initiatives, and other efforts at multiple levels that involve investment in, transition to, or use of cyber technologies (e.g., transition to a zero trust architecture)
- The types of external coordination in which the organization will participate (e.g., consumer of threat intelligence, bi-directional threat information-sharing, cooperation or coordination to counter threats, collaboration)
- Whether and how deception can be used

D.2 CYBER RESILIENCY OBJECTIVES

Table D-1 provides representative examples of sub-objectives for each cyber resiliency objective defined in Table 3. A sub-objective motivates the definition of requirements and the selection and tailoring of controls. The representative sub-objectives can be used as a starting point for eliciting restatements of objectives and for defining metrics, as illustrated in the table. The

[105] See [Bodeau16].

representative sub-objectives, suitably restated for the system-of-interest, can be further decomposed into capabilities of (or activities performed by) that system, and threshold and objective values can be stated.[106]

TABLE D-1: CYBER RESILIENCY SUB-OBJECTIVES

OBJECTIVE	REPRESENTATIVE SUB-OBJECTIVES	REPRESENTATIVE EXAMPLES OF METRICS
PREVENT OR AVOID **Definition:** Preclude the successful execution of an attack or the realization of adverse conditions.	• Apply basic protection measures and controls tailored to the risks of the system-of-interest. • Limit exposure to threat events. • Decrease the adversary's perceived benefits. • Modify configurations based on threat intelligence.	• Time to patch or to apply configuration changes. • Percentage of resources for which configuration changes are randomly made. Percentage of resources for which lifespan limits are applied. • Percentage of sensitive data assets that are encrypted. Adversary dwell time in a deception environment. • Percentage of resources to which more restrictive privileges are automatically applied in response to threat indicators.
PREPARE **Definition:** Maintain a set of realistic courses of action that address predicted or anticipated adversity.	• Create and maintain cyber courses of action. • Maintain the resources needed to execute cyber courses of action. • Validate the realism of cyber courses of action using testing or exercises.	• Number of cyber courses of action (CCoAs) in the cyber playbook. Percentage of identified threat types, categories of threat actions, or TTPs (with reference to an identified threat model) addressed by at least one CCoA in the cyber playbook. • Percentage of cyber resources that are backed up. Time since the last exercise of alternative communications paths. Percentage of administrative staff who have been trained in their CCoA responsibilities. • Time since last (random, scheduled) exercise or simulation of one or more CCoAs.
CONTINUE **Definition:** Maximize the duration and viability of essential mission or business functions during adversity.	• Minimize the degradation of service delivery. • Minimize interruptions in service delivery. • Ensure that ongoing functioning is correct.	• Time to perform mission or business function damage assessment. Length of time performance of specified mission or business function remained below acceptable levels. • Time from initial disruption to availability (at minimum level of acceptability) of essential functions. • Percentage of essential data assets for which data quality has been validated. Percentage of essential processing services for which correctness of functioning has been validated.
CONSTRAIN **Definition:** Limit damage from adversity.	• Identify potential damage. • Isolate resources to limit future or further damage. • Move resources to limit future or further damage.	• Percentage of critical components that employ anti-tamper, shielding, and power line filtering. Time from initial indication or warning to completion of scans for potentially damaged resources.

[106] See [Bodeau18b].

OBJECTIVE	REPRESENTATIVE SUB-OBJECTIVES	REPRESENTATIVE EXAMPLES OF METRICS
	• Change or remove resources and how they are used to limit future or further damage.	• Time from initial indication or warning to the completion of component isolation. • Time from initial indication or warning to the completion of resource relocation. • Time from initial indication or warning to the completion of switch to an alternative.
RECONSTITUTE **Definition:** Restore as much mission or business functionality as possible after adversity.	• Identify untrustworthy resources and damage.[107] • Restore functionality. • Heighten protections during reconstitution. • Determine the trustworthiness of restored or reconstructed resources.	• Time to identify unavailable resources and represent damage in status visualization. • Time between the initiation of recovery procedures and the completion of documented milestones in the recovery, contingency, or continuity of operations plan. Percentage of cyber resources for which access control is maintained throughout the recovery process. • Percentage of cyber resources for which additional auditing or monitoring is applied during and after the recovery process. Time to bring a backup network intrusion detection system online. Percentage of reconstituted cyber resources that are placed in a restricted enclave for a period after reconstitution. • Percentage of restored or reconstructed (mission-critical, security-critical, supporting) data assets for which data integrity/quality is checked.
UNDERSTAND **Definition:** Maintain useful representations of mission and business dependencies and the status of resources with respect to possible adversity.	• Understand adversaries. • Understand dependencies on and among systems containing cyber resources. • Understand the status of resources with respect to threat events. • Understand the effectiveness of security controls and controls supporting cyber resiliency.	• Time between the receipt of threat intelligence and the determination of its relevance. Adversary dwell time in deception environment. • Time since the most recent refresh of mission dependency or functional dependency map. Time since the last cyber table-top exercise, Red Team exercise, or execution of controlled automated disruption. • Percentage of system elements for which failure or the indication of potential faults can be detected. Percentage of cyber resources monitored. • Number of attempted intrusions stopped at a network perimeter. Average length of time to recover from incidents.
TRANSFORM **Definition:** Modify mission or business	• Redefine mission or business process threads for agility. • Redefine mission or business functions to mitigate risks.	• Percentage of mission or business process threads that have been analyzed with respect to common dependencies and potential single points of failure. Percentage

[107] Damage need not be identified with specific resources. For example, degraded service can be systemic. Resources (e.g., processes) can be untrustworthy even if they appear to be performing correctly.

OBJECTIVE	REPRESENTATIVE SUB-OBJECTIVES	REPRESENTATIVE EXAMPLES OF METRICS
functions and supporting processes to handle adversity and address environmental changes more effectively.		of mission or business process threads for which alternative courses of action are documented. • Percentage of essential functions for which no dependencies on resources shared with nonessential functions can be identified. Percentage of problematic data feeds to which risk mitigations have been applied since last analysis.
RE-ARCHITECT **Definition:** Modify architectures to handle adversity and address environmental changes more effectively.	• Restructure systems or sub-systems to reduce risks. • Modify systems or sub-systems to reduce risks.	• Size of the (hardware, software, supply chain, user, privileged user) attack surface. Percentage of system components for which provenance can be determined. Percentage of system components that can be selectively isolated. • Percentage of cyber resources for which custom analytics have been developed. Percentage of mission-critical components for which one or more custom-built alternatives are implemented.

D.3 CYBER RESILIENCY TECHNIQUES

This section provides definitions for cyber resiliency *techniques*, one of the fundamental cyber resiliency constructs, which also include goals, objectives, approaches, and design principles. The objectives support goals, the techniques support objectives, the approaches support techniques, and the design principles support the realization of the goals and objectives. The relationship among the cyber resiliency constructs, including specific mapping tables for the constructs, is provided in Appendix F. Table D-2 lists each cyber resiliency technique and its purpose. Table D-3 identifies potential interactions (e.g., synergies, conflicts) between cyber resiliency techniques.

TABLE D-2: CYBER RESILIENCY TECHNIQUES

TECHNIQUE	PURPOSE
ADAPTIVE RESPONSE **Definition:** Implement agile courses of action to manage risks.	Optimize the ability to respond in a timely and appropriate manner to adverse conditions, stresses, attacks, or indicators of these, thus maximizing the ability to maintain mission or business operations, limit consequences, and avoid destabilization.
ANALYTIC MONITORING **Definition:** Monitor and analyze a wide range of properties and behaviors on an ongoing basis and in a coordinated way.	Maximize the ability to detect potential adverse conditions; reveal the extent of adverse conditions, stresses, or attacks; identify potential or actual damage, and investigate adversary TTPs. Provide the data needed for situational awareness.

TECHNIQUE	PURPOSE
CONTEXTUAL AWARENESS **Definition:** Construct and maintain current representations of the posture of organizational missions or business functions while considering threat events and courses of action.	Support situational awareness. Enhance understanding of dependencies among cyber and non-cyber resources. Reveal patterns or trends in adversary behavior.
COORDINATED PROTECTION **Definition:** Ensure that protection mechanisms operate in a coordinated and effective manner.	Require an adversary to overcome multiple safeguards (i.e., implement a strategy of defense-in-depth). Increase the difficulty for an adversary to successfully attack critical resources, increasing the cost to the adversary and raising the likelihood of adversary detection. Ensure that the use of any given protection mechanism does not create adverse, unintended consequences by interfering with other protection mechanisms. Validate the realism of cyber courses of action.
DECEPTION **Definition:** Mislead, confuse, hide critical assets from, or expose covertly tainted assets to the adversary.	Mislead, confuse, or hide critical assets from the adversary, thereby making the adversary uncertain of how to proceed, delaying the effect of the attack, increasing the risk of being discovered, causing the adversary to misdirect or waste its resources, and exposing the adversary tradecraft prematurely.
DIVERSITY **Definition:** Use heterogeneity to minimize common mode failures, particularly threat events exploiting common vulnerabilities.	Limit the possibility of the loss of critical functions due to the failure of replicated common components. Cause an adversary to expend more effort by developing malware or other TTPs appropriate for multiple targets; increase the probability that the adversary will waste or expose TTPs by applying them to targets for which they are inappropriate; and maximize the probability that some of the defending organization's systems will survive the adversary's attack.
DYNAMIC POSITIONING **Definition:** Distribute and dynamically relocate functionality or system resources.	Increase the ability to rapidly recover from non-adversarial events (e.g., fires, floods) as well as from cyber attacks. Impede an adversary's ability to locate, eliminate, or corrupt mission or business assets, and cause the adversary to spend more time and effort finding the organization's critical assets, thereby increasing the probability of the adversary revealing their presence, actions, and tradecraft prematurely.
NON-PERSISTENCE **Definition:** Generate and retain resources as needed or for a limited time.	Reduce exposure to corruption, modification, or compromise. Provide a means of curtailing an adversary's intrusion and advance and potentially removing malware or damaged resources from the system. Limit the availability of resources the adversary could target.
PRIVILEGE RESTRICTION **Definition:** Restrict privileges based on the attributes of users and system elements as well as on environmental factors.	Limit the impact and probability that unintended actions by authorized individuals will compromise information or services. Impede an adversary by requiring them to invest more time and effort in obtaining credentials. Curtail the adversary's ability to take full advantage of credentials that they have obtained.
REALIGNMENT **Definition:** Structure systems and resource uses to meet mission or business function needs, reduce current and anticipated risks, and accommodate the evolution of technical, operational, and threat environments.	Minimize the connections between mission-critical and non-critical services, thus reducing the likelihood that a failure of non-critical services will impact mission-critical services. Reduce the attack surface of the defending organization by minimizing the probability that non-mission or business functions could be used as an attack vector. Accommodate changing mission or business function needs. Accommodate changes in the technical environment.

TECHNIQUE	PURPOSE
REDUNDANCY **Definition:** Provide multiple protected instances of critical resources.	Reduce the consequences of the loss of information or services. Facilitate recovery from the effects of an adverse cyber event. Limit the time during which critical services are denied or limited.
SEGMENTATION **Definition:** Define and separate system elements based on criticality and trustworthiness.	Contain adversary activities and non-adversarial stresses (e.g., fires, floods) to the enclave or segment in which they have established a presence. Limit the set of possible targets to which malware can be easily propagated.
SUBSTANTIATED INTEGRITY **Definition:** Ascertain whether critical system elements have been corrupted.	Facilitate the determination of correct results in case of conflicts between diverse services or inputs. Detect attempts by an adversary to deliver compromised data, software, or hardware, as well as successful modification or fabrication.
UNPREDICTABILITY **Definition:** Make changes randomly or unpredictably.	Increase an adversary's uncertainty regarding the system protections that they may encounter, thus making it more difficult for them to ascertain the appropriate course of action. Serve as a force multiplier for other techniques.

2187
2188
2189 **TABLE D-3: POTENTIAL INTERACTIONS BETWEEN CYBER RESILIENCY TECHNIQUES**

Technique / Enabler B Technique A	Adaptive Response	Analytic Monitoring	Contextual Awareness	Coordinated Protection	Deception	Diversity	Dynamic Positioning	Non-Persistence	Privilege Restriction	Realignment	Redundancy	Segmentation	Substantiated Integrity	Unpredictability
ADAPTIVE RESPONSE	-	D	U	S		U	U/S	U/S	U/S		U	U/S	U	U
ANALYTIC MONITORING	S	-	S	D	U	U	U						U/S	
CONTEXTUAL AWARENESS	S	U	-							S			U	
COORDINATED PROTECTION	U	S		-		U	U	U	U/S	U	U	U		
DECEPTION		U/C	C/S		-		U					U	S	U
DIVERSITY	S	C/S	C	C/S		-	S		U	U	U/S		U	S
DYNAMIC POSITIONING	U/S	C/S			S	U	-	U			U			U/S
NON-PERSISTENCE	U/S	C	C				S	-		S			U	S
PRIVILEGE RESTRICTION	S			U					-	S			U	
REALIGNMENT	C		U	C/S		C/S			S	-	C			

Technique / Enabler B Technique A	Adaptive Response	Analytic Monitoring	Contextual Awareness	Coordinated Protection	Deception	Diversity	Dynamic Positioning	Non-Persistence	Privilege Restriction	Realignment	Redundancy	Segmentation	Substantiated Integrity	Unpredictability
REDUNDANCY	S					U	S				-		U	
SEGMENTATION	U/S	C		S	S							-		U
SUBSTANTIATED INTEGRITY	S	S/U	S		U	S		S	S		S		-	
UNPREDICTABILITY	C/S	C		C	S	U	U/S	U						-

Key:
- **S** indicates that the technique in the row (Technique A) *supports* the one in the column (Technique B). Technique B is made more effective by Technique A.
- **D** indicates that Technique A *depends on* Technique or Enabler B. Technique A will be ineffective if not used in conjunction with Technique or Enabler B.
- **U** indicates that Technique A can *use* Technique or Enabler B. Technique A can be implemented effectively in the absence of Technique B. However, more options become available if Technique B is also used.
- **C** indicates that Technique A can *conflict with or complicate* Technique B. Some or all implementations of Technique A could undermine the effectiveness of Technique B.

D.4 CYBER RESILIENCY IMPLEMENTATION APPROACHES

This section identifies representative cyber resiliency *approaches* to implementing cyber resiliency techniques. A cyber resiliency approach is a subset of the technologies and processes included in a cyber resiliency technique and is defined by how the capabilities are implemented or how the intended consequences are achieved. Table D-4 lists each cyber resiliency technique, representative approaches that can be used to implement the technique, and representative examples. Where possible, examples are drawn from discussions associated with the controls and control enhancements in [SP 800-53], even when these controls or enhancements do not directly support cyber resiliency as described in Appendix F. However, [SP 800-53] does not address all approaches or all aspects of any individual approach. Therefore, some examples are drawn from system reliability and system resilience practices and technologies and/or from emerging cyber resiliency technologies. The set of approaches for a specific technique is not exhaustive and represents relatively mature technologies and practices. Thus, technologies emerging from research can be characterized in terms of the techniques they apply while not being covered by any of the representative approaches.

2208 **TABLE D-4: CYBER RESILIENCY APPROACHES**

TECHNIQUES	APPROACHES	EXAMPLES
ADAPTIVE RESPONSE **Definition:** Implement agile courses of action to manage risks. **Discussion:** 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. However, all approaches can also be applied to processes and reporting within a Security Operations Center (SOC).	**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. **Discussion:** Reconfiguration needs to be executed without significantly degrading or interrupting service.	• Dynamically change router rules, access control lists, intrusion detection and prevention system parameters, and filter rules for firewalls and gateways. • Reassign responsibilities among staff within a security operations center (SOC) based on expertise with a technology for which new warnings have been shared.
	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. **Discussion:** Reallocate resources to tasks or functions without terminating critical functions or processes.	• Employ dynamic provisioning. • Reprioritize messages or services. • Implement load-balancing. • Provide emergency shutoff capabilities. • Preempt communications. • Instruct SOC staff to prioritize analysis and response to one incident among multiple suspected incidents.
	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. **Discussion:** Manage how mechanisms can be used based on changes in the operational environment as well as changes in the threat environment.	• Disable access dynamically. • Implement adaptive authentication. • Provide for the automatic disabling of a system or service. • Provide dynamic deployment of new or replacement resources or capabilities. • Use automated decision-making supported by artificial intelligence (AI) or machine learning (ML) for rapid response and dynamic changes when human operators are not available. • Create a temporary incident-focused team reporting structure within an SOC.
ANALYTIC MONITORING **Definition:** Monitor and analyze a wide range of properties and behaviors on an ongoing basis and in a coordinated way. **Discussion:** Systems can accumulate vast amounts of monitoring or logging data. Use monitoring data	**MONITORING AND DAMAGE ASSESSMENT** **Definition:** Monitor and analyze behavior and characteristics of components and resources to look for indicators of adversary activity or precursor conditions or indications of other threat events and to detect and assess damage from adversity. **Informal description:** Look for indications that something might be	• Use hardware fault detection. • Employ Continuous Diagnostics and Mitigation (CDM) or other vulnerability scanning tools. • Deploy intrusion detection systems (IDSs) and other monitoring tools. • Use insider threat monitoring tools. • Perform telemetry analysis. • Detect malware beaconing.

TECHNIQUES	APPROACHES	EXAMPLES
strategically to inform defensive activities.	awry and what damage might have occurred. **Discussion:** Leverage Continuous Diagnostics and Mitigation (CDM) and other monitoring capabilities, including those related to health and status (H&S). Integrate with threat hunting and insider threat monitoring.	• Monitor open-source information for indicators of disclosure or compromise.
	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. **Discussion:** Consider all possible sources of monitoring information, including CDM, H&S, physical access logs, and insider threat monitoring.	• Enable organization-wide situational awareness. • Implement cross-organizational auditing. • Correlate data from different tools. • Fuse data from physical access control systems and information systems.
	FORENSIC AND BEHAVIORAL ANALYSIS **Definition:** Analyze adversary TTPs, including observed behavior, malware, and other artifacts left behind by adverse events. **Informal description:** Analyze adversary activities and artifacts. **Discussion:** Ensure that policies and practices are in place to capture evidence and support analysis.	• Deploy an integrated team of forensic and malware analysts, developers, and operations personnel. • Use reverse engineering and other malware analysis tools.
CONTEXTUAL AWARENESS **Definition:** Construct and maintain current representations of the posture of missions or business functions while considering threat events and courses of action. **Discussion:** Maintain cyber situational awareness to support mission continuity.	**DYNAMIC RESOURCE AWARENESS** **Definition:** Maintain current information about resources, the status of resources, and resource connectivity. **Informal description:** Maintain awareness of systems' performance and security posture. **Discussion:** Integrate network performance, system performance, and continuous diagnostics as part of situational awareness.	• Maintain a real-time network map. • Integrate health and status (H&S) data with outputs of CDM tools.
	DYNAMIC THREAT AWARENESS **Definition:** Maintain current information about threat actors, indicators, and potential, predicted, and observed adverse events.	• Track predicted or impending natural disasters. • Dynamically ingest incident and threat data. • Track ownership changes of suppliers and other depended-on parties.

TECHNIQUES	APPROACHES	EXAMPLES
	Informal description: Maintain a current awareness of threats that are both observed and anticipated. **Discussion:** Ensure that the organization's security operations center (SOC) ingests cyber threat intelligence.	• Facilitate integrated situational awareness of threats.
	MISSION DEPENDENCY AND STATUS VISUALIZATION **Definition:** Maintain current information about 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. **Discussion:** 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.	• Maintain a mission-wide or organization-wide operational picture or dashboard. • Maintain a current security posture assessment for critical resources or high-value assets.
COORDINATED PROTECTION **Definition:** Ensure that protection mechanisms operate in a coordinated and effective manner. **Discussion:** 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:** Do not expect one defense to suffice. Apply layered defenses based on risk. **Discussion:** Avoid creating single points of failure.	• Design for defense-in-depth. • Employ multiple, distinct authentication challenges over the course of a session to confirm identity. • Combine network and host-based intrusion detection. • Provide increasing levels of protection to access more sensitive or critical resources. • Conduct sensitivity and criticality analyses.
	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. **Discussion:** Over time, changing access policies for information, allowable uses of capabilities, and dependencies among systems and	• Employ unified Identity, Credential, and Access Management (ICAM) administration tools. • Analyze mission and business process flows and threads. • Employ privilege analysis tools to support an ongoing review of whether user privileges are assigned consistently. • Interpret attributes consistently. • Use machine learning for access control policy verification [IR 8360].

TECHNIQUES	APPROACHES	EXAMPLES
	components can produce fragility and provide adversaries with opportunities.	• Design for facilitating coordination and mutual support among safeguards.
	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 system components to avoid coverage gaps or interference. **Discussion:** Orchestrate updates of capabilities and policies, particularly, for identity, credentialing, and access management (ICAM) across systems. Orchestrate monitoring across architectural layers. Use a cyber playbook to orchestrate incident response efforts.	• Coordinate incident handling with mission and business process continuity of operations and organizational processes. • Coordinate the planning, training, and testing of incident response, contingency planning, etc. • Make software updates in a consistent, coordinated way across the organization. • Deploy ICAM policy updates in a consistent, coordinated way across the organization. • Conduct coverage planning and management for sensors. • Use cyber playbooks.
	SELF-CHALLENGE **Definition:** Affect mission or business processes or system elements adversely in a controlled manner to validate the effectiveness of protections and enable proactive response and improvement. **Informal description:** Validate the effectiveness of capabilities and processes in action. **Discussion:** Use tabletop exercises (TTXs), Red Teams, penetration testing, or automated fault injection throughout the system life cycle and with different scopes.	• Hardware power-on self-test. • Conduct role-based training exercises. • Conduct penetration testing and Red Team exercises. • Test automated incident response. • Employ fault injection. • Conduct tabletop exercises.
DECEPTION **Definition:** Mislead, confuse, hide critical assets from, or expose covertly tainted assets to the adversary. **Discussion:** Apply deception strategically, tactically, or both. Ensure that cyber risk governance and SOC operations allow for	**OBFUSCATION** **Definition:** Hide, transform, or otherwise obscure the contents, properties, or presence of information or other assets from the adversary. **Informal description:** Make information difficult for the adversary to find and understand. **Discussion:** Encryption is a key method for obfuscation.	• Encrypt data at rest. • Use steganographic encoding (e.g., digital watermarking). • Encrypt transmitted data (e.g., using a Virtual Private Network [VPN]). • Encrypt authenticators. • Randomize communications patterns. • Conceal the presence of system components on an internal network.

TECHNIQUES	APPROACHES	EXAMPLES
deception, and maintain deception resources.		• Mask, encrypt, hash, or replace identifiers. • Obfuscate traffic via onion routing. • Apply chaffing to communications traffic. • Add a large amount of valid but useless information to a data store. • Perform encrypted processing.
	DISINFORMATION **Definition:** Provide deliberately misleading information to adversaries. **Informal description:** Deceive adversaries. **Discussion:** Typical forms of disinformation include decoy accounts and decoy credentials.	• Post questions to a public forum based on false information about the system. • Create false ("canary") credentials and tokens (e.g., honeytokens).
	MISDIRECTION **Definition:** Maintain deception resources or environments, and direct adversary activities there. **Informal description:** Direct adversary activities to deception environments or resources. **Discussion:** 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.	• Establish and maintain honeypots, honeynets, or decoy files. • Maintain a full-scale, all-encompassing deception environment.
	TAINTING **Definition:** Embed covert capabilities in resources. **Informal description:** Cause what adversaries steal to identify them or otherwise harm them. **Discussion:** Enable exfiltrated data to "phone home."	• Use beacon traps. • Employ internal network table cache poisoning (e.g., Domain Name System [DNS], Address Resolution Protocol [ARP]). • Include false entries or steganographic data in files to enable them to be found via open-source analysis.
DIVERSITY **Definition:** Use heterogeneity to minimize common mode failures, particularly threat events that exploit common vulnerabilities. **Discussion:** Enterprise systems often include some incidental diversity as a result of procurements by different programs or at different	**ARCHITECTURAL DIVERSITY** **Definition:** Use multiple sets of technical standards, different technologies, and different architectural patterns. **Informal description:** Use different technical architectures. **Discussion:** An organization can use, for example, both Windows and Linux. An organization's cloud	• Use auditing/logging systems on different OSs to acquire and store audit/logging data. • Apply different audit/logging regimes at different architectural layers. • Deploy diverse operating systems. • Support multiple protocol standards. • [Non-cyber example] Use both airplanes and lighter-than-air aircraft for air transportation.

TECHNIQUES	APPROACHES	EXAMPLES
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.	strategy can involve multiple cloud infrastructures.	
	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. **Discussion:** Within the context of a given architecture, parallel design teams can solve the same problem in different ways, thus producing different attack surfaces.	• Employ N-version programming. • Employ mixed-signal design diversity (using both analog and digital signals). • Employ mixed-level design diversity (using both hardware and software implementations). • [Non-cyber example] Use both helium-filled and hot air dirigibles.
	SYNTHETIC DIVERSITY **Definition:** Transform implementations of software to produce a variety of instances. **Informal description:** Use automation to tweak software implementations. **Discussion:** Synthetic diversity can be applied to IoT devices.	• Implement address space layout randomization. • Use randomizing compilers.
	INFORMATION DIVERSITY **Definition:** Provide information from different sources or transform information in different ways. **Informal description:** Use multiple sources for the same information. **Discussion:** Use of information from different sources can reveal adversary injection or modification.	• Apply different analog-to-digital conversion methods to non-digitally-obtained data. • Use multiple data sources.
	PATH DIVERSITY **Definition:** Provide multiple independent paths for command, control, and communications. **Informal description:** Do not rely on a single mode of communication. **Discussion:** In particular, ensure alternative lines of communications for incident response and continuity of an organization's essential functions.	• Establish alternate telecommunications services (e.g., ground-based circuits, satellite communications). • Employ alternate communications protocols. • Use out-of-band channels.
	SUPPLY CHAIN DIVERSITY **Definition:** Use multiple independent supply chains for critical components. **Informal description:** Look for ways to avoid relying on a single supply chain.	• Use a diverse set of suppliers. • Analyze components from different suppliers to determine whether they contain common elements (e.g., included software libraries).

TECHNIQUES	APPROACHES	EXAMPLES
	Discussion: Determine when and how to use supply chain diversity as part of the organization's SCRM strategy.	
DYNAMIC POSITIONING **Definition:** Distribute and dynamically relocate functionality or system resources. **Discussion:** 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. **Discussion:** Relocating sensors compensates for blind spots and makes it harder for an adversary to hide.	• Relocate (using virtualization) or reconfigure IDSs or IDS sensors.
	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. **Discussion:** Make the adversary's discovery and network mapping efforts go stale quickly.	• Change processing locations (e.g., switch to a virtual machine on a different physical component). • Change storage sites (e.g., switch to an alternate data store on a different storage area network).
	ASSET MOBILITY **Definition:** Securely move physical resources. **Informal description:** Do not confine physical resources to one location. **Discussion:** This approach is applicable to cyber-physical and tactical systems.	• Move a mobile device or system component (e.g., a router) from one room in a facility to another while monitoring its movement. • Move storage media securely from one room or facility to another room or facility. • Move a platform or vehicle to avoid collision or other physical harm while retaining knowledge of its location.
	FRAGMENTATION **Definition:** Partition information and distribute it across multiple components. **Informal description:** Create an information jigsaw puzzle. **Discussion:** Manage fragmented data to ensure its ongoing quality, minimize its exposure, and minimize performance inefficiencies.	• Strategically implement data fragmentation and partitioning to maintain performance while ensuring quality.
	DISTRIBUTED FUNCTIONALITY **Definition:** Decompose a function or application into smaller functions, and	• Architect applications so that constituent functions can be located on different system components.

TECHNIQUES	APPROACHES	EXAMPLES
	distribute those functions across multiple components. **Informal description:** Use fine-grained control of resource use. **Discussion:** Distributed functionality can be used with micro-segmentation and ZTA.	
NON-PERSISTENCE **Definition:** Generate and retain resources as needed or for a limited time. **Discussion:** 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. **Discussion:** Determine how temporary "temporary" files are.	• Delete high-value mission information after it is processed. • Offload audit records to offline storage. • Use one-time passwords or nonces.
	NON-PERSISTENT SERVICES **Definition:** Refresh services periodically, or generate services on demand and terminate services when no longer needed. **Informal description:** Do not allow a service to run indefinitely. It may have been compromised while executing. **Discussion:** Instantiating services on demand and expunging them when inactive can be a performance management strategy as well.	• Employ time-based or inactivity-based session termination. • Reimage components. • Refresh services using virtualization.
	NON-PERSISTENT CONNECTIVITY **Definition:** Establish connections on demand, and terminate connections when no longer needed. **Informal description:** Do not leave a communications line open. **Discussion:** Leverage software-defined networking (SDN), particularly in a ZTA.	• Implement software-defined networking. • Employ time-based or inactivity-based network disconnection.
PRIVILEGE RESTRICTION **Definition:** Restrict privileges based on attributes of users and system elements as well as on environmental factors. **Discussion:** Apply existing capabilities more stringently, and integrate ZT technologies.	**TRUST-BASED PRIVILEGE MANAGEMENT** **Definition:** Define, assign, and maintain privileges based on established trust criteria consistent with the principles of least privilege. **Informal description:** Trust no more than necessary. **Discussion:** Separate roles and responsibilities, and use dual authorization.	• Implement least privilege. • Employ location-based account restrictions. • Employ time-based restrictions on automated processes. • Require dual authorization for critical actions.
	ATTRIBUTE-BASED USAGE RESTRICTION	• Employ role-based access control (RBAC).

TECHNIQUES	APPROACHES	EXAMPLES
	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. **Discussion:** Avoid treating a system or an application as a Swiss Army knife.	• Employ attribute-based access control (ABAC). • Restrict the use of maintenance tools. • Apply asset tag policy restrictions to the use of cloud services. • Use dynamic data masking.
	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. **Discussion:** Make access and usage decisions based on the current state and recent history.	• Implement time-based adjustments to privileges due to the status of mission or business tasks. • Employ dynamic account provisioning. • Disable privileges based on a determination that an individual or process is high-risk. • Implement dynamic revocation of access authorizations. • Implement dynamic association of attributes with cyber resources and active entities. • Implement dynamic credential binding.
REALIGNMENT **Definition:** Structure systems and resource uses to meet mission or business function needs, reduce current and anticipated risks, and accommodate the evolution of the technical, operational, and threat environments. **Discussion:** Look for restructuring opportunities related to new systems and programs, as well as planned upgrades to existing systems.	**PURPOSING** **Definition:** Ensure that cyber resources are used consistently with mission or business function purposes and approved uses, thereby avoiding unnecessary sharing and complexity. **Informal description:** Ensure that resources are used consistently with mission or business function purposes and approved uses. **Discussion:** Avoid "mission creep," which can increase a system's attack surface.	• Use allow-listing to prevent the installation of unapproved applications, such as games or peer-to-peer music sharing. • Use allow-listing to restrict communications to a specified set of addresses. • Ensure that privileged accounts are not used for non-privileged functions. • Ensure that no resource is designated as trusted unless a mission or business reason justifies that designation.
	OFFLOADING **Definition:** Offload supportive but nonessential 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. **Discussion:** Offloading reduces the attack surface and motivates ongoing consideration of what is essential.	• Outsource nonessential services to a managed service provider. • Impose requirements on and perform oversight of external system services.

TECHNIQUES	APPROACHES	EXAMPLES
	RESTRICTION **Definition:** Remove or disable unneeded functionality or connectivity, or add mechanisms to reduce the chance of vulnerability or failure. **Informal description:** Lock capabilities down. **Discussion:** Lock capabilities down even though that reduces agility and leaves some capabilities unused.	• Configure the system to provide only essential capabilities. • Minimize non-security functionality.
	REPLACEMENT **Definition:** Replace low-assurance or poorly understood implementations with trustworthy implementations. **Informal description:** Replace those components that cannot be trusted. **Discussion:** In certain circumstances, it is best to discard components, particularly in light of supply chain risks. However, the decommissioning and replacement processes need to be secure.	• Remove or replace unsupported system components to reduce risk.
	SPECIALIZATION **Definition:** Uniquely augment, configure, or modify the design of critical cyber resources for missions or business functions to improve trustworthiness. **Informal description:** Build special-purpose components or develop non-standard implementations. **Discussion:** Prevent the adversary from being able to mirror your system.	• Reimplement or custom develop critical components. • Develop custom system elements covertly. • Define and apply customized configurations.
	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:** Do not commit to a static architecture or an architecture that is difficult to change. **Discussion:** Expect a broader range of "plug and play" capabilities over time.	• Use function, driver, and object wrappers to facilitate the rapid removal and replacement of components. • Use microservices to support incremental changes. • Use virtualization to enable new or different applications and OSs to be installed rapidly. • Integrate ongoing training into mission or business processes to accommodate change.
REDUNDANCY	**PROTECTED BACKUP AND RESTORE** **Definition:** Back up information and software (including configuration data	• Retain previous baseline configurations.

TECHNIQUES	APPROACHES	EXAMPLES
Definition: Provide multiple protected instances of critical resources. **Discussion:** Redundancy is integral to system resilience, but it must be carefully managed to avoid redundant vulnerabilities and an increased attack surface.	and virtualized resources) in a way that protects its confidentiality, integrity, and authenticity. Enable safe and secure restoration in case of disruption or corruption. **Informal description:** Back up resources securely and defend the restore process from adversary exploitation. **Discussion:** Keep in mind that transitions are often periods of exposure, and backups can be compromised.	• Maintain and protect system-level backup information (e.g., operating system, application software, system configuration data). • Increase monitoring and analysis during restore operations.
	SURPLUS CAPACITY **Definition:** Maintain extra capacity for information storage, processing, or communications. **Informal description:** Do not economize on resources; provide surge capacity. **Discussion:** Where possible, use diverse resources to provide surplus capacity.	• Maintain spare parts (i.e., system components). • Address surplus capacity in service-level agreements with external systems.
	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. **Discussion:** Where possible, replicate capabilities using diverse resources.	• Provide an alternate audit capability. • Create a shadow database. • Maintain one or more alternate storage sites. • Maintain one or more alternate processing sites. • Maintain a redundant secondary system. • Provide alternative security mechanisms. • Implement a redundant name and address resolution service.
SEGMENTATION **Definition:** Define and separate system elements based on criticality and trustworthiness. **Discussion:** 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. **Discussion:** Predefined enclaves and micro-segmentation facilitate the risk-calibrated use of other security and cyber resiliency techniques.	• Use virtualization to maintain separate processing domains based on user privileges. • Use cryptographic separation for maintenance. • Partition applications from system functionality. • Isolate security functions from non-security functions. • Use physical separation (air gap) to isolate security tools and capabilities. • Isolate components based on organizational missions or business functions.

TECHNIQUES	APPROACHES	EXAMPLES
		• Separate subnets that connect to different security domains. In particular, provide a DMZ for Internet connectivity. • Use cross-domain solutions to separate security domains. • Employ system partitioning. • Implement micro-segmentation using software agents. • Employ process isolation. • Implement sandboxes and other confined environments. • Implement memory protection.
	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. **Discussion:** The use of dynamic segmentation and isolation, consistent with ZT principles, can be particularly useful for high-value assets.	• Implement dynamic isolation of components. • Implement software-defined networking (SDN), network function virtualization (NFV), and VPNs to define new enclaves. • Create a virtualized sandbox or detonation chamber for untrusted attachments or URLs.
SUBSTANTIATED INTEGRITY **Definition:** Ascertain whether critical system elements have been corrupted. **Discussion:** Verify that critical system elements can be trusted and have not been subjected to tampering or other malicious activity.	**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. **Discussion:** Integrity checks can be applied to information, metadata, components, or services.	• Use tamper-evident seals and anti-tamper coatings. • Use automated tools for data quality checking. • Use blockchain technology. • Use non-modifiable executables. • Use polling techniques to identify potential damage. • Implement cryptographic hashes to address the modification of checksums as well as data. • Validate the trustworthiness of a cloud server platform before launching a container worker node and periodically during container runtime execution. • Employ information input validation. • Validate components as part of SCRM. • Employ integrity checking on external systems.

TECHNIQUES	APPROACHES	EXAMPLES
	PROVENANCE TRACKING **Definition:** Identify and track the provenance of data, software, or hardware elements. **Informal description:** Verify the source of the system elements on which the organization depends. **Discussion:** Make provenance tracking part of SCRM.	• Employ component traceability as part of SCRM. • Employ provenance tracking as part of SCRM. • Implement anti-counterfeit protections. • Implement a trusted path. • Implement code signing.
	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. **Discussion:** Learn what activities or behaviors are normal and what activities or behaviors are suspicious. Coordinate with insider threat mitigation.	• Employ detonation chambers. • Implement function verification. • Verify boot process integrity. • Implement fault injection to observe potential anomalies in error handling.
UNPREDICTABILITY **Definition:** Make changes randomly or unpredictably. **Discussion:** Maintain an environment of uncertainty for the adversary. Keep the adversary guessing.	**TEMPORAL UNPREDICTABILITY** **Definition:** Change behavior or state at times that are determined randomly or by complex functions. **Informal description:** Keep the adversary from extrapolating from past events. **Discussion:** Do not let the present conditions or circumstances duplicate the past.	• Require reauthentication at random intervals. • Perform routine actions at different times of the day.
	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. **Discussion:** Do not let the adversary take advantage of consistency.	• Rotate roles and responsibilities. • Implement random channel-hopping. • Use random masking in dynamic data masking.

As the examples in Table D-4 illustrate, cyber resiliency techniques and approaches can be applied at a variety of architectural layers or system elements, including elements of the technical system (e.g., hardware, networking, software, and information stores) and system elements that are part of the larger socio-technical system: operations (e.g., people and

processes supporting cyber defense, system administration, and mission or business function tasks), support (e.g., programmatic, systems engineering, maintenance and support), and environment of operation (e.g., physical access restrictions and physical location). For a representative set of architectural layers, Table D-5 indicates approaches that could be applied at those layers. In Table D-5, "other software" includes specialized software intended to implement cyber resiliency or cybersecurity capabilities. Some approaches (e.g., Calibrated Defense-in-Depth, Consistency Analysis) can involve working across multiple layers or at multiple locations.

TABLE D-5: ARCHITECTURAL LAYERS AT WHICH CYBER RESILIENCY APPROACHES CAN BE USED

		SOCIO-TECHNICAL SYSTEM										
		TECHNICAL SYSTEM								OPERATIONS	SUPPORT	ENVIRONMENT OF OPERATION
		HARDWARE AND FIRMWARE	NETWORKING AND COMMUNICATIONS	SOFTWARE				INFORMATION STORAGE MANAGEMENT	TECHNICAL SYSTEM AS A WHOLE			
				OTHER SOFTWARE	OPERATING SYSTEM	CLOUD, VIRTUALIZATION MIDDLEWARE, INFRASTRUCTURE	APPLICATION					
TECHNIQUES	**APPROACHES**											
ADAPTIVE RESPONSE	**Dynamic Reconfiguration**	X	X		X	X	X		X	X		
	Dynamic Resource Allocation		X		X	X	X		X	X		
	Adaptive Management		X		X		X		X	X		
ANALYTIC MONITORING	**Monitoring and Damage Assessment**		X	X					X	X		
	Sensor Fusion and Analysis		X	X	X				X	X		
	Forensic and Behavioral Analysis			X					X	X		
COORDINATED PROTECTION	**Calibrated Defense-in-Depth**								X	X	X	
	Consistency Analysis			X					X	X	X	
	Orchestration					X			X	X		
	Self-Challenge	X	X	X	X		X			X		

TECHNIQUES	APPROACHES	SOCIO-TECHNICAL SYSTEM										
		TECHNICAL SYSTEM								OPERATIONS	SUPPORT	ENVIRONMENT OF OPERATION
		HARDWARE AND FIRMWARE	NETWORKING AND COMMUNICATIONS	SOFTWARE				INFORMATION STORAGE MANAGEMENT	TECHNICAL SYSTEM AS A WHOLE			
				OTHER SOFTWARE	OPERATING SYSTEM	CLOUD, VIRTUALIZATION MIDDLEWARE, INFRASTRUCTURE	APPLICATION					
CONTEXTUAL AWARENESS	**Dynamic Resource Awareness**		X	X					X	X		
	Dynamic Threat Awareness			X					X	X		
	Mission Dependency and Status Visualization			X					X	X		
DECEPTION	**Obfuscation**	X	X	X	X		X	X		X	X	
	Disinformation						X	X		X	X	
	Misdirection		X	X					X	X	X	
	Tainting		X	X			X					
DIVERSITY	**Architectural Diversity**	X	X	X	X	X	X					
	Design Diversity	X	X	X	X	X	X					
	Synthetic Diversity				X	X	X					
	Information Diversity							X		X		
	Path Diversity		X							X		
	Supply Chain Diversity	X									X	
DYNAMIC POSITIONING	**Functional Relocation of Sensors**		X	X	X	X			X	X		
	Functional Relocation of Cyber Resources		X	X	X	X	X		X	X		
	Asset Mobility									X		X
	Fragmentation							X				
	Distributed Functionality			X		X	X		X	X		

TECHNIQUES	APPROACHES	SOCIO-TECHNICAL SYSTEM										
		TECHNICAL SYSTEM								OPERATIONS	SUPPORT	ENVIRONMENT OF OPERATION
		HARDWARE AND FIRMWARE	NETWORKING AND COMMUNICATIONS	SOFTWARE				INFORMATION STORAGE MANAGEMENT	TECHNICAL SYSTEM AS A WHOLE			
				OTHER SOFTWARE	OPERATING SYSTEM	CLOUD, VIRTUALIZATION MIDDLEWARE, INFRASTRUCTURE	APPLICATION					
NON-PERSISTENCE	**Non-Persistent Information**				X	X	X	X		X		
	Non-Persistent Services				X	X			X			
	Non-Persistent Connectivity		X						X	X		X
PRIVILEGE RESTRICTION	**Trust-Based Privilege Management**			X	X		X		X			
	Attribute-Based Usage Restriction	X	X	X	X		X		X			
	Dynamic Privileges			X	X		X		X			
REALIGNMENT	**Purposing**		X	X	X		X			X	X	
	Offloading			X			X			X		
	Restriction		X	X	X		X			X	X	
	Replacement	X		X							X	
	Specialization	X		X			X				X	
	Evolvability		X	X		X	X		X	X	X	
REDUNDANCY	**Protected Backup and Restore**			X	X		X	X	X	X		
	Surplus Capacity	X	X			X	X	X		X		
	Replication	X	X			X	X	X	X	X		
SEGMENTATION	**Predefined Segmentation**	X	X	X	X	X		X		X		X
	Dynamic Segmentation and Isolation	X	X	X	X	X				X		X
	Integrity Checks	X	X	X	X	X	X	X		X		

TECHNIQUES	APPROACHES	SOCIO-TECHNICAL SYSTEM										
		TECHNICAL SYSTEM								OPERATIONS	SUPPORT	ENVIRONMENT OF OPERATION
		HARDWARE AND FIRMWARE	NETWORKING AND COMMUNICATIONS	SOFTWARE				INFORMATION STORAGE MANAGEMENT	TECHNICAL SYSTEM AS A WHOLE			
				OTHER SOFTWARE	OPERATING SYSTEM	CLOUD, VIRTUALIZATION MIDDLEWARE, INFRASTRUCTURE	APPLICATION					
SUBSTANTIATED INTEGRITY	**Provenance Tracking**	X	X		X		X	X			X	
	Behavior Validation	X	X	X	X	X	X			X		
UNPREDICTABILITY	**Temporal Unpredictability**		X	X	X	X	X			X		
	Contextual Unpredictability		X	X	X	X	X			X		

D.5 CYBER RESILIENCY DESIGN PRINCIPLES

This section provides a description of *strategic* and *structural* cyber resiliency design principles—key constructs in the cyber resiliency engineering framework. It also describes relationships with the design principles from other disciplines, the analytic practices necessary to implement the principles, and how the application of the principles affects risk. In particular, relationships to security design principles as described in [SP 800-160 v1] are identified.[108] As noted in Section 2.1.4, strategic design principles express the organization's risk management strategy, and structural design principles support the strategic design principles.

D.5.1 Strategic Design Principles

Strategic cyber resiliency design principles guide and inform engineering analyses and risk analyses throughout the system life cycle and highlight different structural design principles, cyber resiliency techniques, and approaches to applying those techniques. Table D-6 describes

[108] [SP 800-160 v1] defines security design principles in three broad categories: Security Architecture and Design, Security Capability and Intrinsic Behaviors, and Life Cycle Security. For a detailed discussion of relationships between security design principles and cyber resiliency techniques as well as cyber resiliency design principles, see [Bodeau17].

2237 five strategic cyber resiliency design principles and identifies the related design principles from
2238 other disciplines.[109] [110]

2239 **TABLE D-6: STRATEGIC CYBER RESILIENCY DESIGN PRINCIPLES**

STRATEGIC DESIGN PRINCIPLES	KEY IDEAS	RELATED DESIGN PRINCIPLES FROM OTHER DISCIPLINES
FOCUS ON COMMON CRITICAL ASSETS.	**Motivation:** 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 that are both critical and common followed by those that are either critical or common. **Guidance:** Know which mission or business functions, tasks, capabilities, and assets are critical. Know which resources, assets, or services are essential to the successful performance of critical functions and tasks or to the protection of critical assets. Focus first on ensuring the security and cyber resiliency of those essential resources that are common across multiple functions as high-value adversary targets.	**Security:** Inverse Modification Threshold. **Resilience Engineering:** Physical Redundancy, Layered Defense, Loose Coupling. **Survivability:** Failure Mode Reduction, Fail-Safe, Evolution.

[109] Resilience Engineering design principles are described in the Systems Engineering Body of Knowledge [SEBoK] and [Jackson13]. Resilience Engineering design principles mapped to cyber resiliency design principles in this appendix are: Absorption (allow the system to withstand threats to a specified level), Human-in-the-Loop (allow the system to employ human elements when there is a need for human cognition), Internode Interaction (allow the nodes of the system to communicate, cooperate, and collaborate with other nodes when this interaction is essential), Modularity (construct the system of relatively independent but interlocking system components or system elements; also called Localized Capacity), Neutral State (allow the system to incorporate time delays that will allow human operators to consider actions to prevent further damage), Complexity Avoidance (incorporate features that enable the system to limit its own complexity to a level not more than necessary), Hidden Interactions Avoidance (incorporate features that assure that potentially harmful interactions between nodes are avoided), Redundancy [functional] (employ an architecture with two or more independent and identical branches), Redundancy [physical] (employ an architecture with two or more different branches; also called Diversity), Loose Coupling (construct the system of elements that depend on each other to the least extent practicable), Defense-in-Depth (provide multiple means to avoid failure; also called Layered Defense), Restructuring (incorporate features that allow the system to restructure itself; also known as Reorganization), and Reparability (incorporate features that allow the system to be brought up to partial or full functionality over a specified period of time and in a specified environment).

[110] Survivability design principles are described in [Richards08]. The Survivability design principles mapped to cyber resiliency design principles in this appendix are: Prevention (suppress a future or potential future disturbance); Mobility (relocate to avoid detection by an external change agent), Concealment (reduce the visibility of a system from an external change agent), Deterrence (dissuade a rational external agent from committing a disturbance), Preemption (suppress an imminent disturbance), Avoidance (maneuver away from an ongoing disturbance), Hardness (resist deformation), Redundancy (duplicate critical system functions to increase reliability), Margin (allow extra capabilities to maintain value delivery despite losses), Heterogeneity (vary system elements to mitigate homogeneous disturbances), Distribution (separate critical system elements to mitigate local disturbances), Failure Mode Reduction (eliminate system hazards through intrinsic design: substitute, simplify, decouple, and reduce hazardous materials), Fail-Safe (prevent or delay degradation via physics of incipient failure), Evolution (alter system elements to reduce disturbance effectiveness), Containment (isolate or minimize the propagation of failure), Replacement (substitute system elements to improve value delivery), and Repair (restore the system to improve value delivery).

STRATEGIC DESIGN PRINCIPLES	KEY IDEAS	RELATED DESIGN PRINCIPLES FROM OTHER DISCIPLINES
SUPPORT AGILITY AND ARCHITECT FOR ADAPTABILITY.	**Motivation:** 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. **Guidance:** Prepare for changes in the technical, operational, and threat environments. Leverage existing and emerging standards to support interoperability. Recognizing that the organization could invest in capabilities or create programs for varying purposes and with different time frames, manage risks due to dependencies or other interactions among programs or initiatives.	**Security:** Secure Evolvability, Minimized Sharing, Reduced Complexity, Secure System Modification. **Resilience Engineering:** Reorganization, Human Backup, Inter-Node Interaction. **Survivability:** Mobility, Evolution.
REDUCE ATTACK SURFACES.	**Motivation:** A large attack surface is difficult to defend and requires 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. **Guidance:** Understand the organization's attack surfaces—not only the exposed elements of systems but also people and processes. Consider how an adversary could attack development, operational, and maintenance environments. Consider attack surfaces in the cyber supply chain. Consider social media exposure and insider threats.	**Security:** Least Common Mechanism, Minimized Sharing, Reduced Complexity, Minimized Security Elements, Least Privilege, Predicate Permission. **Resilience Engineering:** Complexity Avoidance, Drift Correction. **Survivability:** Prevention, Failure Mode Reduction.
ASSUME COMPROMISED RESOURCES.	**Motivation:** 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. **Guidance:** Structure systems and mission or business processes to minimize the harm that could result from a specific	**Security:** Trusted Components, Self-Reliant Trustworthiness, Trusted Communications Channels. *Incompatible with Security:* Hierarchical Protection. **Resilience Engineering:** Human Backup, Localized Capacity, Loose Coupling.

STRATEGIC DESIGN PRINCIPLES	KEY IDEAS	RELATED DESIGN PRINCIPLES FROM OTHER DISCIPLINES
	product or type of technology being compromised. Consider the potential for lateral movement by an adversary as well as for cascading failures. Analyze and prepare to manage the potential consequences of learning that a key component, service, or technology has been compromised or found vulnerable.	
EXPECT ADVERSARIES TO EVOLVE.	**Motivation:** Advanced cyber adversaries invest time, effort, and intelligence-gathering to improve existing TTPs 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 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. **Guidance:** Incorporate an adversarial perspective when analyzing architectural changes, design modifications, and changes in operational procedures and governance structures. Use cyber threat intelligence (CTI), but do not be limited by it—take a longer-term view, and expect the threat landscape to continue to change.	**Security:** Trusted Communications Channels. **Resilience Engineering:** Reorganization, Drift Correction. **Survivability:** Evolution.

Strategic design principles are driven by an organization's risk management strategy and, in particular, by its risk framing. Risk framing may include assumptions about the threats the organization should be prepared for, the constraints on risk management decision-making (including which risk response alternatives are irrelevant), and organizational priorities and trade-offs.[111] From the standpoint of cyber resiliency, one way to express priorities is in terms of which cyber resiliency objectives are most important. Each strategic design principle supports the achievement of one or more cyber resiliency objectives and relates to the design principles, concerns, or analysis processes associated with other specialty engineering disciplines. The relationships between strategic cyber resiliency design principles, risk framing, and analytic practices are indicated in Table D-7. Relationships between design principles and other cyber resiliency constructs are identified in Section D.6.

[111] See [SP 800-39].

2254 **TABLE D-7: STRATEGIC DESIGN PRINCIPLES DRIVE ANALYSIS AND RELATE TO RISK MANAGEMENT**

STRATEGIC DESIGN PRINCIPLES AND ANALYTIC PRACTICES	RISK FRAMING ELEMENTS OF RISK MANAGEMENT STRATEGY
FOCUS ON COMMON CRITICAL ASSETS. ***Practices*:** Criticality Analysis, Business Impact Analysis (BIA), Mission Impact Analysis (MIA), Mission Thread Analysis	**Threat assumptions:** Conventional adversary; advanced adversary seeking path of least resistance **Risk response constraints:** Limited programmatic resources **Risk response priorities:** Anticipate, Withstand, Recover
SUPPORT AGILITY AND ARCHITECT FOR ADAPTABILITY. ***Practices*:** Analysis of standards conformance, interoperability analysis, reusability analysis	**Threat assumptions:** Adaptive, agile adversary **Risk response constraints:** Missions to be supported and mission needs can change rapidly **Risk response priorities:** Recover, Adapt
REDUCE ATTACK SURFACES. ***Practices*:** Supply Chain Risk Management (SCRM) analysis, vulnerability and exposure analysis, Operations Security (OPSEC) analysis, Cyber attack modeling and simulation	**Threat assumptions:** Conventional adversary; advanced adversary seeking path of least resistance **Risk response constraints:** Limited operational resources to monitor and actively defend systems **Risk response priorities:** Anticipate
ASSUME COMPROMISED RESOURCES. ***Practices*:** Cascading failure analysis, Insider Threat analysis, Cyber attack modeling and simulation	**Threat assumptions:** Advanced adversary **Risk response constraints:** Ability to assure the trustworthiness of system elements is limited **Risk response priorities:** Anticipate, Withstand
EXPECT ADVERSARIES TO EVOLVE. ***Practices*:** Adversary-driven Cyber Resiliency (ACR) analysis, Red Teaming	**Threat assumptions**: Advanced adversary; adversary can change TTPs and goals unpredictably **Risk response priorities**: Anticipate, Adapt

2255
2256
2257 Sections D.5.1.1 through D.5.1.5 provide descriptions of the *strategic* cyber resiliency principles.

2258 ### *D.5.1.1 Focus on Common Critical Assets*

2259 A focus on critical assets (i.e., resources valued due to their importance to mission or business
2260 accomplishment)[112] is central to contingency planning, continuity of operations planning,
2261 operational resilience, and safety analysis. Critical assets can be identified using a variety of
2262 mission-oriented analysis techniques, including Mission Impact Analysis (MIA), Business Impact
2263 Analysis (BIA),[113] Functional Dependency Network Analysis (FDNA), Crown Jewels Analysis (CJA),
2264 and Mission Thread Analysis. In some instances, failure modes, effects, and criticality analysis
2265 (FMECA) can reflect a safety-oriented approach.

2266 Assets that are common to multiple missions or business functions are potential high-value
2267 targets for adversaries either because those assets are critical or because their compromise
2268 increases the adversaries' options for lateral motion[114] or persistence [OMB M-19-03]. Once an
2269 asset is identified as critical or common, further analysis involves:

[112] Critical assets may also be referred to as high-value assets (HVA) in accordance with [OMB M-19-03].

[113] See [SP 800-34].

[114] Lateral motion refers to an adversary's ability to move transitively from one system element to another system element or in a system-of-systems from one constituent system to another constituent system.

- Identifying how the asset is used in different operational contexts (e.g., normal operations, abnormal operations, crisis or emergency operations, failover). An asset that is common to multiple missions may be critical to one mission in one context but not in a second or critical to a second mission only in the second context.
- Determining which properties or attributes make the asset critical (e.g., correctness, non-observability, availability) or high value (e.g., providing access to a set of critical system elements, providing information that could be used in further malicious cyber activities) and what would constitute an acceptable (e.g., safe, secure) failure mode. Again, properties that are critical to one mission may be nonessential to another, and a failure mode that is acceptable from the standpoint of security may be unacceptable from the standpoint of safety.
- Determining which strategies to use to ensure critical properties, taking into consideration the different usage contexts and potential malicious cyber activities. Strategies for ensuring the correctness and non-observability properties include disabling non-critical functionality, restoring to default or known-good settings, and selectively isolating or disabling data flows to or from system components. Articulating trade-offs among critical properties and acceptable failure modes is central to effective risk management.

Based on the strategy or strategies that best fit a given type of asset, the most appropriate or relevant structural design principles can be determined.

This strategic design principle makes common infrastructures (e.g., networks), shared services (e.g., identity and access management services), and shared data repositories high priorities for the application of selected cyber resiliency techniques. It recognizes that the resources for risk mitigation are limited and enables systems engineers to focus resources where they will have the greatest potential impact on risk mitigation.

D.5.1.2 Support Agility and Architect for Adaptability

In Resilience Engineering, *agility* means "the effective response to opportunity and problem, within a mission" [Jackson07] [Sheard08]. In that context, resilience supports agility and counters brittleness. In the context of cyber resiliency, agility is the property of an infrastructure or a system that can be reconfigured, in which components can be reused or repurposed, and in which resources can be reallocated so that cyber defenders can define, select, and tailor cyber courses of action (CCoA) for a broad range of disruptions or malicious cyber activities. This strategy is consistent with the vision that the "infrastructure allows systems and missions to be reshaped nimbly to meet tactical goals or environment changes" [King12]. Agility enables the system and operational processes to incorporate new technologies and/or adapt to changing adversary capabilities.

Adaptability is the property of an architecture, a design, and/or an implementation that can accommodate changes to the threat model, mission or business functions, technologies, and systems without major programmatic impacts. A variety of strategies for agility and adaptability have been defined. These include modularity and controlled interfaces to support plug-and-play, the externalization of rules and configuration data, and the removal or disabling of unused components to reduce complexity. Application of this design principle early in the system life cycle can reduce sustainment costs and modernization efforts.

This design principle means that analyses of alternative architectures and designs need to search for sources of brittleness (e.g., reliance on a single operating system or communications channel, allowing single points of failure, reliance on proprietary interface standards, use of large and hard-to-analyze multi-function modules). Therefore, the analyses need to focus on Realignment and consider Redundancy, Adaptive Response, Diversity, and the Coordinated Protection capabilities that enable cyber defenders to make effective use of these techniques. In addition, analyses need to consider where and how to use "cyber maneuver," or moving target defenses, and Deception. Finally, analyses need to consider where and how an architecture, design, or as-deployed system is bound to designated assumptions about the threat, operational, and/or technical environments.

D.5.1.3 Reduce Attack Surfaces

The term *attack surface* refers to the set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from that system, system element, or environment. The system's attack surface can be characterized as the accessible areas where weaknesses or deficiencies (including in hardware, software, and firmware system components) provide opportunities for adversaries to exploit vulnerabilities [SP 800-53] or as its exposure to reachable and exploitable vulnerabilities: any hardware, software, connection, data exchange, service, or removable media that might expose the system to potential threat access [DOD15].

Some uses of the term focus on externally exposed vulnerabilities (i.e., the attack surface of a system that connects to a network includes access control points for remote access). However, the assumption that an adversary will penetrate an organization's systems means that internal exposures (i.e., vulnerabilities that can be reached by lateral movement within a system or infrastructure) are also part of the attack surface. Conceptually, the term *attack surface* can also cover aspects of the development, operational, and maintenance environments that an adversary can reach and that could contain vulnerabilities. The supply chain for a system can also present additional attack surfaces. More broadly, an organization can be said to have an attack surface that includes its personnel, external users of organizational systems (if any), and its supply chain both for mission or business operations and information and communications technology (ICT). To accommodate these broader interpretations of the term, the design principle refers to "attack surfaces."

This design principle is often used in conjunction with the Focus on common critical assets principle. Analysis of internal attack surfaces can reveal unplanned and unexpected paths to critical assets. It makes the identification or discovery of attack surfaces a priority in system design analyses,[115] as well as analyses of development, configuration, and maintenance environments (e.g., by considering how using free and open-source software [FOSS] or commercial off-the-shelf [COTS] products that cannot be tailored in those environments expands attack surfaces). It may be infeasible in some architectures (e.g., Internet of Things, bring-your-own-device) or procurement environments (e.g., limited supply chain) for which the Assume compromised resources principle is highly relevant.

[115] For example, [SP 800-53] control SA-11(6), Developer Security Testing | Attack Surface Reviews, calls for the analysis of design and implementation changes.

As indicated in Table D-8, several alternative strategies for reducing an attack surface can be identified. These strategies are expressed by different controls in [SP 800-53] and apply different cyber resiliency techniques. In Table D-8, the **bolding** in the discussion of the control indicates how the control supports the strategy. These strategies can be reflected by different structural principles. For example, design decisions related to the Maximize transience and Change or disrupt the attack surface structural principles can reduce the duration of exposure; application of the Limit the need for trust principle can reduce exposure. While the controls in Table D-8 focus on attack surfaces within a system, the strategies apply more broadly to the attack surfaces of a mission or an organization. For example, Operations Security (OPSEC) can reduce exposure of the mission or organization to adversary reconnaissance. Supply chain protections can reduce the exposure of key components to tampering.

TABLE D-8: STRATEGIES FOR REDUCING ATTACK SURFACES[116]

STRATEGY	SECURITY CONTROL SUPPORTING STRATEGY	RELATED TECHNIQUES
REDUCE THE EXTENT OF THE ATTACK SURFACE.	Attack surface reduction includes **implementing the concept of layered defenses, applying the principles of least privilege and least functionality, deprecating unsafe functions, and applying secure software development practices, including reducing entry points available to unauthorized users, reducing the amount of code that executes, and eliminating application programming interfaces (APIs) that are vulnerable to cyber attacks**. SA-15(5) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION [SP 800-53]	Coordinated Protection Privilege Restriction Realignment
REDUCE THE EXPOSURE (STRUCTURAL ACCESSIBILITY) OF THE ATTACK SURFACE.	Attack surface reduction includes **implementing the concept of layered defenses and applying the principles of least privilege and least functionality**. SA-15(5) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION [SP 800-53]	Privilege Restriction Coordinated Protection
	Component isolation reduces the attack surface of organizational systems. SC-7(20) BOUNDARY PROTECTION | DYNAMIC ISOLATION AND SEGREGATION [SP 800-53]	Adaptive Response Segmentation
REDUCE THE DURATION (TEMPORAL ACCESSIBILITY) OF ATTACK SURFACE EXPOSURE.	The implementation of non-persistent components and services mitigates risk from advanced persistent threats (APTs) by reducing the targeting capability of adversaries (i.e., **window of opportunity** and available attack surface) to initiate and complete attacks. SI-14 NON-PERSISTENCE [SP 800-53]	Non-Persistence

This design principle in conjunction with the Support agility and architect for adaptability principle motivates analyses of the effects on the attack surface of a system-of-interest due to changes in its overall environment. Analyses consider changes in the organizational, operational,

[116] The security control supporting strategy includes examples and excerpts from relevant [SP 800-53] controls.

and programmatic environments, which can change physical, supply chain, personnel, technical, and procedural aspects of the attack surface, as well as technical aspects.

D.5.1.4 Assume Compromised Resources

A significant number of system architectures treat many, if not all, resources as non-malicious. This assumption is particularly prevalent in cyber-physical systems (CPS) and Internet of Things (IoT) architectures [Folk15]. However, systems and their components, ranging from chips to software modules to running services, can be compromised for extended periods without detection [DSB13]. In fact, some compromises may never be detected. Thus, the assumption that some system resources have been compromised is prudent. While the assumption that some resources cannot be trusted is well-established from the standpoint of security (i.e., the compromised resources cannot be trusted to follow established security policies), the concept of trustworthiness is broader. By compromising a resource, an adversary can affect its reliability, the ability to enforce other policies, or the safety of the larger system or environment of which the resource is a part or can use the resource in an attack on other systems [SP 1500-201] NIST16].

This design principle implies the need for analysis of how the system architecture reduces the potential consequences of a successful compromise—in particular, the duration and degree of adversary-caused disruption and the speed and extent of malware propagation. An increasing number of modeling and simulation techniques support the analysis of the potential systemic consequences stemming from the compromise of a given resource or set of resources. Such analysis includes identifying different types or forms of systemic consequences (e.g., unreliable or unpredictable behavior of services, unreliable or unpredictable availability of capabilities, or data of indeterminate quality) and subsequently linking these systemic consequences to mission consequences (e.g., mission failure, safety failure) or organizational consequences (e.g., loss of trust or reputation).

D.5.1.5 Expect Adversaries to Evolve

Advanced cyber adversaries invest time, effort, and intelligence-gathering to improve existing TTPs 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. This design principle supports a risk management strategy that includes and goes beyond the common practice of searching for and seeking ways to remediate known vulnerabilities (or classes of vulnerabilities). A system that has been hardened in the sense of remediating known vulnerabilities will remain exposed to evolving adversaries.

This design principle implies the need for analyses in which the adversary perspective is explicitly represented by intelligent actors who can play the role of an adaptive or evolving adversary. For implemented systems, such analyses are typically part of *red teaming* or *war gaming*. Analyses can use threat intelligence or repositories of attack patterns (e.g., ATT&CK [MITRE18], CAPEC [MITRE07]) to provide concrete examples, but care should be taken not to be constrained by those examples. Voice of the Adversary (VoA) is a design analysis technique in which one or more team members play the role of an adversary to critique alternatives by taking into consideration possible goals, behaviors, and cyber effects assuming varying degrees

of system access or penetration. This type of design analysis can use models or taxonomies of adversary behaviors (e.g., the cyber attack life cycle or cyber kill chain models [Hutchins11], CAPEC [MITRE07] or ATT&CK [MITRE18] classes) and languages or taxonomies of cyber effects (e.g., [Temin10]).

This design principle also highlights the value of the Deception and Diversity techniques. Deception can cause adversaries to reveal their TTPs prematurely from the perspective of their cyber campaign plans, enabling defenders to develop countermeasures or defensive TTPs. Diversity can force an adversary to develop a range of TTPs to achieve the same objectives.

D.5.2 Structural Design Principles

Structural cyber resiliency design principles guide and inform design and implementation decisions throughout the system life cycle. As indicated in Table D-9, many of the structural design principles are consistent with or leverage the design principles for security and/or resilience.[117] The first four design principles are closely related to protection strategies and security design principles and can be applied in mutually supportive ways. The next three design principles are closely related to design principles for resilience engineering and survivability; are driven by the concern for an operational environment (including cyber threats), which changes on an ongoing basis; and are closely related to design principles for evolvability. The final four principles are strongly driven by the need to manage the effects of malicious cyber activities, even when those activities are not observed. Descriptions of how structural design principles are applied or could be applied to a system-of-interest can help stakeholders understand how their concerns are being addressed.

TABLE D-9: STRUCTURAL CYBER RESILIENCY DESIGN PRINCIPLES

STRUCTURAL DESIGN PRINCIPLES	KEY IDEAS	RELATED DESIGN PRINCIPLES FROM OTHER DISCIPLINES
LIMIT THE NEED FOR TRUST.	Limiting the number of system elements that need to be trusted (or the length of time for which an element needs to be trusted) reduces the level of effort needed for assurance, ongoing protection, and monitoring.	**Security:** Least Common Mechanism, Trusted Components, Inverse Modification Threshold, Minimized Security Elements, Least Privilege, Predicate Permission, Self-Reliant Trustworthiness, Trusted Communications Channels. **Resilience Engineering:** Localized Capacity, Loose Coupling. **Survivability:** Prevention.
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.	**Security:** Clear Abstraction, Least Common Mechanism, Least Privilege, Predicate Permission. **Resilience Engineering:** Localized Capacity, Loose Coupling. **Survivability:** Concealment, Hardness.
CONTAIN AND EXCLUDE BEHAVIORS.	Limiting what can be done and where actions can be taken reduces the possibility or extent of the spread of	**Security:** Trusted Components, Least Privilege, Predicate Permission.

[117] The relationship between strategic and structural cyber resiliency design principles is presented in Table D-10.

STRUCTURAL DESIGN PRINCIPLES	KEY IDEAS	RELATED DESIGN PRINCIPLES FROM OTHER DISCIPLINES
	compromises or disruptions across components or services.	**Resilience Engineering:** Localized Capacity, Loose Coupling. **Survivability:** Preemption, Hardness, Distribution.
LAYER DEFENSES AND PARTITION RESOURCES.	The combination of defense-in-depth and partitioning increases the effort required by an adversary to overcome multiple defenses.	**Security:** Modularity and Layering, Partially Ordered Dependencies, Minimized Sharing, Self-Reliant Trustworthiness, Secure Distributed Composition. **Resilience Engineering:** Layered Defense. **Survivability:** Hardness, Fail-Safe
PLAN AND MANAGE DIVERSITY.	Diversity is a well-established resilience technique that removes single points of attack or failure. However, architectures and designs should take cost and manageability into consideration to avoid introducing new risks.	**Resilience Engineering:** Absorption, Repairability. **Survivability:** Heterogeneity.
MAINTAIN REDUNDANCY.	Redundancy is key to many resilience strategies but can degrade over time as configurations are updated or connectivity changes.	**Resilience Engineering:** Absorption, Physical Redundancy, Functional Redundancy. **Survivability:** Redundancy, Margin.
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.	**Resilience Engineering:** Localized Capacity, Repairability. **Survivability:** Mobility, Avoidance, Distribution.
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.	**Resilience Engineering:** Drift Correction, Inter-Node Interaction.
MAINTAIN SITUATIONAL AWARENESS.	Situational awareness, including the awareness of possible performance trends and the emergence of anomalies, informs decisions about cyber courses of action to ensure mission completion.	**Resilience Engineering:** Drift Correction, Inter-Node Interaction.
MANAGE RESOURCES (RISK-) ADAPTIVELY.	Risk-adaptive management supports agility and provides supplemental risk mitigation throughout critical operations despite disruptions or outages of components.	**Security:** Trusted Components, Hierarchical Trust, Inverse Modification Threshold, Secure Distributed Composition, Trusted Communications Channels, Secure Defaults, Secure Failure and Recovery. **Resilience Engineering:** Reorganization, Repairability, Inter-Node Interaction. **Survivability:** Avoidance.

STRUCTURAL DESIGN PRINCIPLES	KEY IDEAS	RELATED DESIGN PRINCIPLES FROM OTHER DISCIPLINES
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.	**Resilience Engineering:** Localized Capacity, Loose Coupling. **Survivability:** Avoidance.
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 and trigger responses such as closer monitoring, more restrictive privileges, or quarantine.	**Security:** Self-Reliant Trustworthiness, Continuous Protection, Secure Metadata Management, Self-Analysis, Accountability and Traceability. **Resilience Engineering:** Neutral State. **Survivability:** Fail-Safe.
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.	**Resilience Engineering:** Drift Correction **Survivability:** Mobility, Deterrence, Preemption, Avoidance.
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.	**Security:** Efficiently Mediated Access, Performance Security, Human Factored Security, Acceptable Security. **Survivability:** Concealment.

The selection of structural design principles is driven by strategic design principles, as shown in Table D-10.

TABLE D-10: 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		

Structural design principles provide guidance for design decisions intended to reduce risk.[118] This guidance affects the selection and the application of cyber resiliency techniques. Table D-15 describes the relationship between structural design principles and cyber resiliency techniques. Table D-11 briefly describes the structural design principles and identifies the intended effects of each structural design principle on risk.

TABLE D-11: STRUCTURAL DESIGN PRINCIPLES AND EFFECTS ON RISK

STRUCTURAL DESIGN PRINCIPLES	INTENDED EFFECTS ON RISK
LIMIT THE NEED FOR TRUST.	Reduce the likelihood of harm due to malice, error, or failure. **Discussion:** Limit the number of system elements that need to be trusted (or the length of time an element needs to be trusted). This reduces the level of effort needed for assurance, ongoing protection, and monitoring. This principle is consistent with ZT tenets.
CONTROL VISIBILITY AND USE.	Reduce the likelihood of occurrence of adversarial events; reduce the likelihood of harm due to malice, error, or failure. **Discussion:** Control what can be discovered, observed, and used. This increases the effort needed by an adversary seeking to expand a foothold or increase impacts. This principle is consistent with ZT tenets.

[118] Harm to a cyber resource can take the form of degradation or disruption of functionality or performance; exfiltration or exposure of information; modification, corruption, or fabrication of information (including software, mission or business information, and configuration data); or usurpation or misuse of system resources. Unless otherwise specified, all forms of harm to systems containing cyber resources are addressed.

STRUCTURAL DESIGN PRINCIPLES	INTENDED EFFECTS ON RISK
CONTAIN AND EXCLUDE BEHAVIORS.	Reduce the likelihood of occurrence of adversarial events; reduce the likelihood of harm due to malice, error, or failure. **Discussion:** Limit what and where actions can be taken. This reduces the possibility or extent of the spread of compromises or disruptions across components or services. This principle is consistent with ZT tenets.
LAYER DEFENSES AND PARTITION RESOURCES.	Reduce the likelihood of harm due to malice, error, or failure; reduce the extent of harm. **Discussion:** The combination of defense-in-depth and partitioning increases the effort required by an adversary to overcome multiple defenses. This principle is consistent with ZT tenets.
PLAN AND MANAGE DIVERSITY.	Reduce the likelihood of harm due to malice, error, or failure; reduce the extent of disruption. **Discussion:** Diversity is a well-established system resilience technique that removes single points of attack or failure. However, it can also increase attack surfaces. The development of architectures and designs should take cost and complexity into consideration to identify and manage new risks.
MAINTAIN REDUNDANCY.	Reduce the likelihood of harm due to malice, error, or failure; reduce the extent of disruption or degradation. **Discussion:** Redundancy is key to many system resilience strategies but can degrade over time as configurations are updated or connectivity changes.
MAKE RESOURCES LOCATION-VERSATILE.	Reduce the likelihood of occurrence of adversarial events; reduce the extent of disruption or degradation. **Discussion:** 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.
LEVERAGE HEALTH AND STATUS DATA.	Reduce the likelihood of harm due to malice, error, or failure by enabling responses to changes in system state; reduce the extent of harm by enabling the detection of and response to indicators of damage. **Discussion:** 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.
MAINTAIN SITUATIONAL AWARENESS.	Reduce the likelihood of harm due to malice, error, or failure by enabling responses to indicators; reduce the extent of harm by enabling the detection of and response to indicators of damage. **Discussion:** Situational awareness, including awareness of possible performance trends and the emergence of anomalies, informs decisions about cyber courses of action to ensure mission completion.

STRUCTURAL DESIGN PRINCIPLES	INTENDED EFFECTS ON RISK
MANAGE RESOURCES (RISK-) ADAPTIVELY.	Reduce the likelihood of harm due to malice, error, or failure by enabling responses to changes in the operational environment; reduce the extent of harm. **Discussion:** Risk-adaptive management supports agility and provides supplemental risk mitigation throughout critical operations despite disruptions or outages of components.
MAXIMIZE TRANSIENCE.	Reduce the likelihood of occurrence by reducing the time during which an adverse event could occur; reduce the likelihood of harm due to malice, error, or failure by reducing the time during which an event could result in harm. **Discussion:** The use of transient system elements (e.g., data, services, connectivity) minimizes the duration of exposure to adversary activities. Periodically refreshing to a known (secure) state can expunge malware or corrupted data.
DETERMINE ONGOING TRUSTWORTHINESS.	Reduce the likelihood of harm due to corrupted, modified, or fabricated information by enabling untrustworthy information to be identified; reduce the extent of harm by reducing the propagation of untrustworthy information. **Discussion:** Do not assume that the properties of a resource, service, process, or connection are stable over time. Perform periodic or ongoing verification and/or validation of properties related to trustworthiness, and perform ongoing monitoring and analysis of behavior. This principle is consistent with ZT tenets.
CHANGE OR DISRUPT THE ATTACK SURFACE.	Reduce the likelihood of occurrence by removing the circumstances in which an adversarial event is feasible; reduce the likelihood of harm due to adversarial events by making such events ineffective. **Discussion:** Disruption of the attack surface can cause the adversary to waste resources, make incorrect assumptions about the system or the defender, prematurely launch attacks, or disclose information.
MAKE THE EFFECTS OF DECEPTION AND UNPREDICTABILITY USER-TRANSPARENT.	Reduce the likelihood of the occurrence of errors; when Deception techniques are applied, reduce the likelihood of the occurrence of adversarial events. **Discussion:** 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.

Sections D.5.2.1 through D.5.2.14 provide more detailed descriptions of the 14 structural cyber resiliency principles.

D.5.2.1 Limit the Need for Trust

Trustworthiness can be defined as a state in which an entity is worthy of being trusted to fulfill whatever critical requirements may be needed for a component, subsystem, system, network, application, mission, enterprise, or other entity [Neumann04]. Trustworthiness has also been defined as the attribute of an entity that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned

responsibilities [CNSSI 4009]. Assertions of trustworthiness (e.g., "this software can be relied upon to enforce the following security policies with a high level of confidence") are meaningless without some form of verification, validation, or demonstration (e.g., design analysis, testing). In the absence of some credible form of assurance (which can be costly and invalidated by changes in the system or the environment), assertions of trustworthiness constitute assumptions. Reducing the size of the set of trusted entities (whether individuals, software components, or hardware components) by minimizing assumptions about what is or can be trusted reduces the attack surface and lowers assurance costs.

The application of this design principle is most effective early in the system life cycle when the motivation of the Prevent/Avoid objective is clearest. When a system already exists, changes to the operational concept (consistent with the Transform objective) or the system architecture (applying the Re-Architect objective and the Realignment technique) can increase costs. One approach to applying this design principle (using the Coordinated Protection and Privilege Restriction techniques) is through limitations on inheritance so that privileges or access rights associated with one class of system component are not automatically propagated to classes or instances created from the original one. While limitations on inheritance can initially increase the burden on developers or administrators, they can also reduce the complexity associated with multiple inheritance.

This design principle supports the strategic design principles of Reduce attack surfaces and Assume compromised resources. However, its application increases the difficulty of applying the Support agility and architect for adaptability strategic design principle. This design principle can also be used in conjunction with Determine ongoing trustworthiness. If a system element is assumed or required to have a given level of trustworthiness, some attestation mechanism is needed to verify that it has and continues to retain that trustworthiness level. Minimizing the number of elements with trustworthiness requirements reduces the level of effort involved in determining ongoing trustworthiness. Finally, this design principle can be used in conjunction with Plan and manage diversity. The managed use of multiple sources of system elements, services, or information can enable behavior or data quality to be validated by comparison.

D.5.2.2 Control Visibility and Use

Controlling visibility counters adversary attempts at reconnaissance from outside or within the system. Thus, the adversary must exert greater effort to identify potential targets, whether for exfiltration, modification, or disruption. Ther visibility of data can be controlled by mechanisms such as encryption, data hiding, or data obfuscation. Visibility into how some resources are used can also be controlled directly, such as by adding chaff to network traffic. Visibility into the supply chain, development process, or system design can be limited via operations security (OPSEC), deception [Heckman15], and split or distributed design and manufacturing. Process obfuscation is an area of active research. An increasing number and variety of deception technologies (e.g., deception nets) can be applied at the system level.

Controlling use counters adversary activities and actions in the *Control*, *Execute*, and *Maintain* phases of the cyber attack life cycle [MITRE18]. To limit visibility or control use, access to system resources can be controlled from the perspectives of multiple security disciplines, including physical, logical (see the discussion of privileges below), and hybrid (e.g., physical locations in a geographically distributed system or in a complex, embedded system). Restrictions on access and use can be guided by information sensitivity, as in standard security practices. Restrictions

can also be based on criticality (i.e., the importance to achieving mission objectives). While some resources can be determined to be mission-critical or mission-essential *a priori*, the criticality of other resources can change dynamically. For example, a resource that is vital to one phase of mission processing can become unimportant after that phase is completed.

Many systems or system components provide the capability to define and manage privileges associated with software, services, processes, hardware, communications channels, and individual users. The assignment of privileges should ideally reflect judgments of operational need (e.g., need-to-know, need-to-use) as well as trustworthiness. The restriction of privileges is well established as a security design principle (i.e., least privilege). Privilege restrictions force adversaries to focus efforts on a restricted set of targets, which can be assured (in the case of software), validated (in the case of data), or monitored (in the case of individuals, processes, communications channels, and services). Non-Persistence and Segmentation can also limit visibility. Thus, this principle can be applied in conjunction with the Contain and exclude behaviors and Maximize transience principles.

D.5.2.3 Contain and Exclude Behaviors

The behavior of a system or system element—including what resources it uses, which systems or system elements it interacts with, or when it takes a given action—can vary based on many legitimate circumstances. However, analysis of the organizational missions or business functions and the processes that carry out those missions and functions [SP 800-39] can identify some behaviors that are always unacceptable and others that are acceptable only under specific circumstances. Therefore, excluding behaviors prevents them from having undesirable consequences. Behaviors can be excluded *a priori* with varying degrees of assurance, from removing functionality to restricting functionality or use, with trade-offs between assurance and flexibility. For example, user activity outside of specific time windows can be precluded. In addition, behaviors can be interrupted based on ongoing monitoring when that monitoring provides a basis for suspicion.

Containing behaviors involves restricting the set of resources or system elements that can be affected by the behavior of a given system element. Such restrictions can but do not necessarily involve a temporal aspect. Containment can be achieved *a priori*, via predefined privileges and segmentation. Alternately, or perhaps additionally, Adaptive Response and Dynamic Isolation can be applied. For example, a sandbox or deception environment can be dynamically created in response to suspicious behavior, and subsequent activities can be diverted there.

D.5.2.4 Layer Defenses and Partition Resources

Defense-in-depth is the integration of people, technology, and operations capabilities to establish variable barriers across multiple layers and missions [CNSSI 4009] and is a well-established security strategy. It describes security architectures constructed through the application of multiple mechanisms to create a series of barriers to prevent, delay, or deter an attack by an adversary [SP 800-160 v1]. Multiple mechanisms to achieve the same objective or provide equivalent functionality can be used at a single layer (e.g., different COTS firewalls to separate zones in a DMZ) or at different layers (e.g., detection of suspicious behavior at the application, operating system, and network layers). To avoid inconsistencies that could result in errors or vulnerabilities, such (multiple) mechanisms should be managed consistently.

Layering defenses restricts the adversary's movement vertically in a layered security architecture (i.e., a defense at one layer prevents a compromise at an adjacent layer from propagating). Partitioning (i.e., separating sets of resources into effectively separate systems) with controlled interfaces (e.g., cross-domain solutions) between them restricts the lateral movement of the adversary. Partitioning can limit the adversary's visibility (see Control visibility and use) and serve to Contain and exclude behaviors. Partitioning can be based on policy and administration, as in security domains [SP 800-160 v1], or be informed by the organizational missions or business functions that the system elements in the partition support. Partitions can be implemented physically, logically, at the network layer, or within a platform (e.g., via hard or soft partitioning). Partitioning may involve limiting resource-sharing or making fewer resources common. If resources are replicated, the Maintain redundancy principle should be applied.

D.5.2.5 Plan and Manage Diversity

Diversity (usually in conjunction with Redundancy [Sterbenz14]) is a well-established technique for improving system resilience [Sterbenz10, Höller15]. For cyber resiliency, Diversity avoids the risk of system homogeneity, in which the compromise of one component can propagate to all other similar components. Diversity offers the benefit of providing alternative ways to deliver required functionality so that if a component is compromised, one or more alternative components that provide the same functionality can be used.

Multiple approaches to diversity can be identified. These include architectural diversity; design diversity; synthetic (or automated) diversity;[119] information diversity; diversity of command, control, and communications (C3) paths (including out-of-band communications); geographic diversity;[120] supply chain diversity [SP 800-160 v1] [Bodeau15]; and diversity in operating procedures. In addition, some incidental architectural diversity often results from procurement over time and differing user preferences. Incidental diversity is often more apparent than real (i.e., different products can present significantly different interfaces to administrators or users while incorporating identical components).

However, diversity can be problematic in several ways. First, it can increase the attack surface of the system. Rather than trying to compromise a single component and propagate across all such components, an adversary can attack any component in the set of alternatives, looking for a path of least resistance to establish a foothold. Second, it can increase demands on developers, system administrators, maintenance staff, and users by forcing them to deal with multiple interfaces to equivalent components. This can result in increased system life cycle costs[121] and increase the risk that inconsistencies will be introduced, particularly if the configuration alternatives for the equivalent components are organized differently. Third, diversity can be more apparent than real (e.g., different implementations of the same mission functionality all running on the same underlying operating system, applications that reuse selected software components). Thus, analysis of the architectural approach to using diversity is critical. For embedded systems, some approaches to diversity raise a variety of research challenges. Finally,

[119] Synthetic diversity in conjunction with randomization, a form of Unpredictability, is a form of Moving Target Defense (MTD).

[120] Geographic diversity can be used to support the Make resources location-versatile structural design principle.

[121] These costs have historically been acceptable in some safety-critical systems.

the effectiveness of diversity against adversaries is not an absolute, and an analysis of diversity strategies is needed to determine the best alternative in the context of adversary TTPs.

Given these considerations, this design principle calls for the use of Diversity in system architecture and design to also take manageability into consideration. It also calls for the consideration of diversity in operational processes and practices, including non-cyber alternatives such as out-of-band measures [SP 800-53] for critical capabilities. To reduce cost and other impacts, this design principle is most effective when used in conjunction with the Focus on common critical assets strategic design principle and the Maintain redundancy and Layer and partition defenses structural principles. Measurements related to this design principle can focus on the degree of diversity, the degree of manageability, or both.

D.5.2.6 Maintain Redundancy

Redundancy is a well-established design principle in Resilience Engineering and Survivability [Sterbenz10]. Approaches to Redundancy include surplus capacity and replication (e.g., cold spares, hot or inline spares) and can be implemented in conjunction with backup and failover procedures. It can enhance the availability of critical capabilities but requires that redundant resources be protected.

Because malware can propagate across homogeneous resources, Redundancy for cyber resiliency should be applied in conjunction with Diversity and considered at multiple levels or layers in a layered architecture [Sterbenz14]. However, Redundancy can increase complexity and present scalability challenges when used in conjunction with Diversity.

The extent of Redundancy is established and maintained through analysis that looks for single points of failure and shared resources. Trends to convergence can undermine Redundancy. For example, an organization using Voice over Internet Protocol (VOIP) for its phone system cannot assert alternate communications paths for phone, email, and instant messaging.

Because maintaining surplus capacity or spare components increases system life cycle costs, this design principle is most effective when used in conjunction with the Focus on common critical assets strategic principle, as well as the Plan and manage diversity and Layer and partition defenses structural principles.

D.5.2.7 Make Resources Location-Versatile

Location-versatile resources do not require a fixed location and can be relocated or reconstituted to maximize performance, avoid disruptions, and better avoid becoming a high-value target for an adversary. Different approaches can be used to provide location-versatile resources, including virtualization, replication, distribution (of functionality or stored data), physical mobility, and functional relocation. Replication is a well-established approach for high-availability systems using multiple, parallel processes, and high-availability data (sometimes referred to as data resilience) with database sharding[122] (although this can present security challenges).

[122] A database *shard* is a horizontal partition of data in a database. Each individual partition is referred to as a shard or database shard. Each shard is held on a separate database server instance to spread the load.

Replication and distribution can be across geographic locations, hardware platforms, or (in the case of services) virtual machines. While replication can take the form of redundancy, it can also involve providing ways to reconfigure system resources to provide equivalent functionality. Data virtualization (i.e., data management that enables applications to retrieve and use data without specific knowledge of the location or format) supports distribution and reduces the likelihood that local (persistent and unmaintained) data stores will proliferate. Composable services enable the alternative reconstitution of mission capabilities, and diverse information sources can be used for the alternative reconstitution of mission or business data.

Application of this principle involves the use of Dynamic Positioning, often in conjunction with Redundancy and/or Diversity. This principle supports the Support agility and architect for adaptability strategic principle and can be employed in conjunction with the Maximize transience and Change or disrupt the attack surface structural principles. Some approaches to the reconstitution of mission capabilities can conflict with the Control visibility and use structural principle.

D.5.2.8 Leverage Health and Status Data

In some architectures, many system components are security-unaware, incapable of enforcing a security policy (e.g., an access control policy), and therefore incapable of monitoring policy compliance (e.g., auditing or alerting to unauthorized access attempts). However, most system components provide health and status data to indicate component availability or unavailability for use. These may include components of CPS (particularly components in space systems) and in the emerging IoT. In addition, system components present health and status data to providers (e.g., application or service on a virtual platform in a cloud to a cloud provider) or service-providing components (e.g., application to operating system, device to network) so that the components can allocate and scale resources effectively. Monitoring data, including health and status data, from multiple layers or types of components in the architecture can help identify potential problems early so they can be averted or contained.

As architectural convergence between information technology (IT) and operational technology (OT) or the IoT increases [SP 1500-201], application of this structural principle will support the Expect adversaries to evolve strategic principle. Given the increasing number and variety of "smart" components in the IoT, application of this principle may be driven by the Focus on common critical assets principle. In addition, components can erroneously or maliciously report health and status data by design or due to compromise. Thus, application of this principle may be more effective in conjunction with the Determine ongoing trustworthiness principle.

D.5.2.9 Maintain Situational Awareness

For security and cyber resiliency, situational awareness encompasses awareness of *system elements*, *threats*, and *mission dependencies* on system elements.[123] An awareness of system elements can rely on security status assessments, security monitoring, and performance monitoring and can be achieved in conjunction with the Leverage health and status data design

[123] As a foundational capability of a Security Operations Center (SOC), situational awareness provides "regular, repeatable repackaging and redistribution of the SOC's knowledge of constituency assets, networks, threats, incidents, and vulnerabilities to constituents. This capability goes beyond cyber intel distribution, enhancing constituents' understanding of the cybersecurity posture of the constituency and portions thereof, driving effective decision-making at all levels [Zimmerman14]."

principle. An awareness of threats involves ingesting and using threat intelligence and recognizing that adversaries evolve. An awareness of system elements and threats (via gathered data, correlated data, and processing capabilities) can be centralized or distributed and either enterprise-internal or cross-enterprise (e.g., via a managed security service provider).

An awareness of mission dependencies can be determined *a priori* as part of system design (e.g., using CJA, MIA, or BIA). Alternately or additionally, mission dependencies can be identified during mission operations by tracking and analyzing resource use. This more dynamic approach supports agility, adaptability, and capabilities to Control visibility and use and Contain and exclude behaviors. While cyber situational awareness remains an active area of research, analytic capabilities are increasingly being offered, and cyber situational awareness is maturing through tailored applications in specific environments.

D.5.2.10 Manage Resources (Risk-) Adaptively

Risk-adaptive management has been developed in multiple contexts. Cybersecurity mechanisms include risk-adaptive access control (RAdAC) for systems—highly adaptive cybersecurity services (HACS) that provide such functionalities as penetration testing, incident response, cyber hunting, and risk and vulnerability assessment for programs—and integrated adaptive cyber defense (IACD) for the enterprise and beyond. Strategies for risk-adaptive management include:

- Changing the frequency of planned changes (e.g., resetting encryption keys, switching between operating systems or platforms, or changing the configuration of internal routers)
- Increasing security restrictions (e.g., requiring reauthentication periodically within a single session, two-factor authentication for requests from remote locations, or two-person control on specific actions, increasing privilege requirements based on changing criticality)
- Reallocating resources (e.g., reallocating processing, communications, or storage resources to enable graceful degradation and the repurposing of resources)
- Discarding or isolating suspected system elements (e.g., terminating a service or locking out a user account, diverting communications to a deception environment, or quarantining processing)

Strategies for implementing this design principle can be applied in conjunction with strategies for implementing Control visibility and use (dynamically changing privileges), Contain and exclude behaviors (disabling resources and dynamic isolation), Layer defenses and partition resources (dynamic partitioning), Plan and manage diversity (switching from one resource to an equivalent resource), and Make resources location-versatile (reconstituting resources).

To be *risk*-adaptive, the selection and application of a strategy should be based on situational awareness—that is, management decisions are based on indications of changes in adversary characteristics, characteristics of system elements, or patterns of operational use that change the risk posture of the system or the mission or business function it supports. Alternately, strategies can be applied unpredictably to address unknown risks.

D.5.2.11 Maximize Transience

Non-persistence is a cyber resiliency strategy to Reduce attack surfaces in the temporal dimension. Virtualization technologies, which simulate the hardware and/or software on which

other software executes [SP 800-125B], enable processes, services, and applications to be transient. At the network layer, technologies for network virtualization, network functions virtualization, software-defined networking, and just-in-time connectivity can support non-persistence. Data virtualization provides a strategy for reducing persistent local data stores. As noted above, this principle is synergistic with Make resources location-versatile. Since transient resources can be virtually isolated, this principle can also be used in conjunction with Contain and exclude behaviors.

Logical transient system elements (e.g., processes, files, connections) need to be expunged (i.e., removed in such a way that no data remains on the shared resources).[124] If an executing process or service has been compromised by malicious software that changes its behavior or corrupts the data it offers to other system elements, expunging it—either by bringing it down or by moving it and deleting the prior instance—also mitigates the compromise. This can be done in response to suspicious behavior or be deliberately unpredictable.

In addition, system elements can be made attritable and expendable, such as in the case of unmanned air systems. These physically transient system elements also need mechanisms for ensuring that no data is left behind.

The instantiation of a transient resource depends on being able to Determine ongoing trustworthiness of the resources from which it is constructed. Support for such verification and/or validation can include gold copies of software and configuration data, policy data for network function virtualization, and data quality validation as part of data virtualization.

D.5.2.12 Determine Ongoing Trustworthiness

In the *Command and Control* and *Defense Evasion* phases of the cyber attack life cycle [MITRE18], an adversary can modify system components (e.g., modify software, replace legitimate software with malware), system data (e.g., modify configuration files, fabricate entries in an authorization database, fabricate or delete audit data), or mission or business data (e.g., deleting, changing, or inserting entries in a mission or business database; replacing user-created files with fabricated versions). These modifications enable the adversary to take actions in the *Impact* and *Persistence* phases of the cyber attack life cycle. Periodic or ongoing validation can detect the effects of adversary activities before they become too significant or irremediable.

A variety of Substantiated Integrity mechanisms can be used to identify suspicious changes to properties or behavior. Some behaviors (e.g., the frequency with which a service makes requests, the latency between a request to it and its response, and the size of requests or responses it makes) can be verified or validated by other services. Other behaviors (e.g., processor, memory, disk, or network) can be verified or validated by other system components (e.g., the operating system's task manager). Note that making the behavior capable of being verified or validated can impede the use of unpredictability.

This principle is strongly synergistic with Manage resources (risk-) adaptively. Some changes can trigger the use of Privilege Restriction or Analytic Monitoring mechanisms. Other changes can trigger quarantine via Segmentation. However, such mechanisms can add storage, processing,

[124] See [SP 800-53] controls SC-4 (Information in Shared System Resources) and MP-6 (Media Sanitization).

and transmission overhead. Therefore, this structural principle is most effective in support of the Focus on common critical assets strategic principle.

Ideally, any system element that cannot be determined to be trustworthy—initially via hardware and software assurance processes and subsequently via Substantiated Integrity—should be assumed to be compromised. However, in practice, that assumption is difficult to apply. This principle is consistent with the weaker assumption that some resources will be compromised and calls for mechanisms to detect and respond to evidence of compromise.

Mechanisms to determine trustworthiness need to be applied in a coordinated manner, across architectural layers, among different types of system elements, and (if applicable) with insider threat controls.

D.5.2.13 Change or Disrupt the Attack Surface

Disruption of the attack surface can also lead an adversary to reveal its presence. A growing set of moving target defenses are intended to change or disrupt the attack surface of a system. Moving Target Defense (MTD) is an active area of research and development. MTD can be categorized in terms of the *layer* or level at which the defenses are applied (e.g., software, runtime environment, data, platform, and network). However, MTD can be applied at other layers. For example, when this design principle is used in conjunction with the Make resources location-versatile principle, MTD can also be applied at the physical or geographic levels. MTD is particularly well-suited to cloud architectures [Shetty16] where implementation is at the middleware level.

MTD can also be categorized in terms of strategy: move, morph, or switch. Resources can be moved (e.g., execution of a service can be moved from one platform or virtual machine to another). This approach, which leverages the design principle of Dynamic Positioning, can be used in conjunction with the Make resources location-versatile principle. The terms "cyber maneuver" and MTD are often reserved for morphing—that is, making specific changes to the properties of the data, runtime environment, software, platform, or network [Okhravi13] or by using configuration changes in conjunction with the techniques of Diversity and Unpredictability or randomization [Jajodia11, Jajodia12] rather than including relocation or distribution. Data or software can be morphed using synthetic diversity; the behavior of system elements can be morphed via configuration or resource allocation changes. Morphing can also be part of a Deception strategy. Finally, switching can leverage diversity and distributed resources. Mission applications that rely on a supporting service can switch from one implementation of the service to another. Switching can also be used in conjunction with Deception, as when adversary interactions with the system are switched to a deception environment.

This structural design principle supports the Expect adversaries to evolve strategic principle. It can also support the Reduce attack surfaces strategic principle. Alternately, the principle can support the Assume compromised resources principle. When Unpredictability is part of the way this principle is applied, it should be used in conjunction with the Make the effects of deception and unpredictability user-transparent structural principle.

D.5.2.14 Make Deception and Unpredictability Effects User-Transparent

Deception and unpredictability are intended to increase an adversary's uncertainty about the system's structure and behavior, what effects an adversary might be able to achieve, and what

actions cyber defenders might take in response to suspected malicious cyber-related activities. [Heckman15] provides a detailed discussion of deception and its role in active cyber defense. Deception includes obfuscation, which increases the effort needed by the adversary and can hide mission activities long enough for the mission to complete without adversary disruption. Active deception can divert adversary activities, causing the adversary to waste resources and reveal TTPs, intent, and targeting.

Unpredictability can apply to structure, characteristics, or behavior. Unpredictable structure (e.g., dynamically changing partitions or isolating components) undermines the adversary's reconnaissance efforts. Unpredictable characteristics (e.g., configurations, selection of an equivalent element from a diverse set) force the adversary to develop a broader range of TTPs. Unpredictable behavior (e.g., response latency) increases uncertainty about effects and whether system behavior indicates defender awareness of malicious cyber activities.

Unpredictability and deception can be applied separately and synergistically. These two techniques can be highly effective against advanced adversaries. However, if implemented poorly, deception and unpredictability can also increase the uncertainty of end-users and administrators about how the system will behave. Such user and administrator confusion can reduce overall resilience, reliability, and security. This uncertainty can, in turn, make the detection of unauthorized or suspicious behavior more difficult. This design principle calls for a sound implementation, which makes system behaviors directed at the adversary transparent to end-users and system administrators.

TAILOR DESIGN PRINCIPLES AND APPLY SELECTIVELY

Cyber resiliency design principles are used to help guide analysis and engineering decisions and to help stakeholders understand the rationale for those decisions. Therefore, design principles can be tailored in terms that are meaningful to the purpose and architecture of the *system-of-interest*. For example, the Support agility and architect for adaptability strategic design principle might be tailored for a microgrid that supplies and manages power for a campus as follows:

> *Design microgrid constituent systems in a modular way to accommodate technology and usage concepts, which change at different rates*.

The design principle might not be directly applicable to an implantable medical device, but it can be applied to a system-of-systems of which the device is a constituent system element in conjunction with the security design principle of *secure evolvability*.

Descriptions of how structural design principles apply will reflect the underlying architecture of the system-of-interest. For example, how the Make resources location-versatile design principle applies to a workflow system might depend on how the enterprise architecture incorporates virtualization and cloud services as well as how it provides off-site backup. Alternatively, the description of how the same design principle applies to a satellite constellation might refer to satellite maneuverability.

D.6 RELATIONSHIPS AMONG CYBER RESILIENCY CONSTRUCTS

Sections D.1 through D.5 presented and described the cyber resiliency constructs of goals, objectives, techniques, approaches, and design principles. Table D-12 and Table D-13 illustrate that the mapping between the goals and objectives is many-to-many, as are the mappings between techniques (including the approaches to implementing or applying techniques) and objectives.

TABLE D-12: CYBER RESILIENCY OBJECTIVES SUPPORTING CYBER RESILIENCY GOALS

Objectives \ Goals	ANTICIPATE	WITHSTAND	RECOVER	ADAPT
PREVENT/AVOID	X	X		
PREPARE	X	X	X	X
CONTINUE		X	X	
CONSTRAIN		X	X	
RECONSTITUTE			X	
UNDERSTAND	X	X	X	X
TRANSFORM			X	X
RE-ARCHITECT			X	X

TABLE D-13: TECHNIQUES AND IMPLEMENTATION APPROACHES TO ACHIEVE OBJECTIVES

Techniques/Approaches \ Objectives	Prevent / Avoid	Prepare	Continue	Constrain	Reconstitute	Understand	Transform	Re-Architect
ADAPTIVE RESPONSE	X	X	X	X	X	X		
Dynamic Reconfiguration	X		X	X	X	X		
Dynamic Resource Allocation	X		X	X	X			
Adaptive Management	X	X	X	X	X	X		
ANALYTIC MONITORING			X	X	X	X		
Monitoring and Damage Assessment			X	X	X	X		
Sensor Fusion and Analysis						X		
Forensic and Behavioral Analysis						X		
CONTEXTUAL AWARENESS		X	X		X	X		
Dynamic Resource Awareness		X				X		
Dynamic Threat Awareness						X		

Objectives / Techniques/Approaches	Prevent / Avoid	Prepare	Continue	Constrain	Reconstitute	Understand	Transform	Re-Architect
Mission Dependency and Status Visualization		X	X		X	X		
COORDINATED PROTECTION	X	X	X		X	X	X	X
Calibrated Defense-in-Depth	X	X			X			
Consistency Analysis	X	X			X	X	X	X
Orchestration	X	X	X		X	X	X	X
Self-Challenge		X				X		
DECEPTION	X					X		
Obfuscation	X							
Disinformation	X							
Misdirection	X					X		
Tainting						X		
DIVERSITY	X	X	X	X				X
Architectural Diversity		X	X					X
Design Diversity		X	X					X
Synthetic Diversity	X	X	X	X				
Information Diversity		X	X					X
Path Diversity		X	X					X
Supply Chain Diversity		X	X					X
DYNAMIC POSITIONING	X		X	X	X	X		
Functional Relocation of Sensors					X	X		
Functional Relocation of Cyber Resources	X		X	X				
Asset Mobility	X		X	X				
Fragmentation	X				X			
Distributed Functionality	X				X			
NON-PERSISTENCE	X			X			X	X
Non-Persistent Information	X			X			X	X
Non-Persistent Services	X			X			X	X
Non-Persistent Connectivity	X			X			X	X
PRIVILEGE RESTRICTION	X			X	X			
Trust-Based Privilege Management	X			X				

Techniques/Approaches \ Objectives	Prevent / Avoid	Prepare	Continue	Constrain	Reconstitute	Understand	Transform	Re-Architect
Attribute-Based Usage Restriction	X				X			
Dynamic Privileges	X			X	X			
REALIGNMENT	X						X	X
Purposing	X							X
Offloading							X	X
Restriction							X	X
Replacement							X	X
Specialization							X	X
Evolvability							X	X
REDUNDANCY	X	X	X		X		X	X
Protected Backup and Restore		X	X		X			
Surplus Capacity		X	X					
Replication	X	X	X				X	X
SEGMENTATION	X			X	X			X
Predefined Segmentation	X			X	X			X
Dynamic Segmentation and Isolation	X			X	X			
SUBSTANTIATED INTEGRITY			X	X	X	X		
Integrity Checks			X	X	X	X		
Provenance Tracking			X		X	X		
Behavior Validation			X	X	X	X		
UNPREDICTABILITY	X			X				
Temporal Unpredictability	X			X				
Contextual Unpredictability	X			X				

Section D.5 identifies cyber resiliency design principles. Strategic design principles support achieving cyber resiliency objectives as shown in Table D-14, while structural design principles provide guidance on how to apply cyber resiliency techniques as shown in Table D-15. Some techniques are required by a design principle; these techniques are **bolded**. Other techniques (not bolded) 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.

2813 **TABLE D-14: STRATEGIC DESIGN PRINCIPLES AND CYBER RESILIENCY OBJECTIVES**

Objectives / Strategic Design Principles	Prevent / Avoid	Prepare	Continue	Constrain	Reconstitute	Understand	Transform	Re-Architect
FOCUS ON COMMON CRITICAL ASSETS.	X		X		X	X		X
SUPPORT AGILITY AND ARCHITECT FOR ADAPTABILITY.		X	X		X		X	X
REDUCE ATTACK SURFACES.	X			X		X	X	X
ASSUME COMPROMISED RESOURCES.		X	X	X	X	X	X	X
EXPECT ADVERSARIES TO EVOLVE.		X				X	X	X

2814
2815
2816 **TABLE D-15: STRUCTURAL DESIGN PRINCIPLES AND CYBER RESILIENCY TECHNIQUES**

STRUCTURAL DESIGN PRINCIPLE	RELATED TECHNIQUE
LIMIT THE NEED FOR TRUST.	Coordinated Protection, **Privilege Restriction**, **Realignment**, Substantiated Integrity
CONTROL VISIBILITY AND USE.	Deception, Non-Persistence, **Privilege Restriction**, **Segmentation**
CONTAIN AND EXCLUDE BEHAVIORS.	Analytic Monitoring, Diversity, Non-Persistence, **Privilege Restriction**, **Segmentation**, Substantiated Integrity
LAYER DEFENSES AND PARTITION RESOURCES.	Analytic Monitoring, **Coordinated Protection**, Diversity, Dynamic Positioning, Redundancy, **Segmentation**
PLAN AND MANAGE DIVERSITY.	Coordinated Protection, **Diversity**, Redundancy
MAINTAIN REDUNDANCY.	Coordinated Protection, Diversity, Realignment, **Redundancy**
MAKE RESOURCES LOCATION-VERSATILE.	Adaptive Response, Diversity, **Dynamic Positioning**, Non-Persistence, Redundancy, Unpredictability
LEVERAGE HEALTH AND STATUS DATA.	**Analytic Monitoring**, **Contextual Awareness**, Substantiated Integrity
MAINTAIN SITUATIONAL AWARENESS.	Analytic Monitoring, **Contextual Awareness**
MANAGE RESOURCES (RISK-) ADAPTIVELY.	**Adaptive Response**, Coordinated Protection, Deception, Dynamic Positioning, Non-Persistence, Privilege Restriction, Realignment, Redundancy, Segmentation, Unpredictability
MAXIMIZE TRANSIENCE.	Analytic Monitoring, Dynamic Positioning, **Non-Persistence**, Substantiated Integrity, Unpredictability
DETERMINE ONGOING TRUSTWORTHINESS.	Coordinated Protection, **Substantiated Integrity**
CHANGE OR DISRUPT THE ATTACK SURFACE.	Adaptive Response, Deception, Diversity, **Dynamic Positioning**, **Non-Persistence**, Unpredictability

STRUCTURAL DESIGN PRINCIPLE	RELATED TECHNIQUE
MAKE THE EFFECTS OF DECEPTION AND UNPREDICTABILITY USER-TRANSPARENT.	Adaptive Response, **Coordinated Protection**, Deception, Unpredictability

D.7 APPLICATION OF CYBER RESILIENCY CONSTRUCTS

Cyber resiliency is addressed in conjunction with the closely related concerns of system resilience and security. Engineering analysis for cyber resiliency emphasizes the need to meet system requirements and address stakeholder concerns in the face of the APT. Cyber resiliency focuses on the capabilities used to ensure the accomplishment of organizational missions or business functions, such as to continue minimum essential operations throughout an attack after the adversary has established a presence in the system as opposed to capabilities to harden the system and to keep the adversary out. The cyber resiliency goals of anticipate, withstand, recover, and adapt are oriented toward organizational missions or business functions and thus complement such security objectives as confidentiality, integrity, and availability that apply to information and information systems [SP 800-37]. Similarly, the cyber resiliency objectives complement the cybersecurity functions of identify, protect, detect, respond, and recover that an organization can use to achieve specific cybersecurity outcomes [NIST CSF].

Due to this complementarity, cyber resiliency can also be incorporated into existing security activities and tasks described in the systems life cycle processes in [SP 800-160 v1]. No new processes are needed, nor are any new activities or tasks needed for the existing processes. Several phrases are integral to the statement and elaboration of the activities and tasks in the systems security engineering processes in [SP 800-160 v1]. These include security aspects, security objectives, security models, concept of security function, security criteria, security-driven constraints, security requirements, and security relevance as applied to a variety of terms. To overcome any potential confusion, the tailoring of statements and elaborations to address cyber resiliency will frequently replace the term *security* with *security and cyber resiliency*. Cyber resiliency offers new considerations for these existing processes, activities, and tasks. However, given that the language in the processes is not specific to cyber resiliency, it may not always be obvious how and where cyber resiliency might be injected into the engineering processes. The experience and expertise of systems security engineers can guide and inform the use of the cyber resiliency constructs described in this publication.

SECONDARY EFFECTS OF APPLYING CYBER RESILIENCY CONSTRUCTS

In addition to the first-order effects realized by organizations due to the application of individual cyber resiliency techniques (or combination of techniques) defined in this publication, there may also be beneficial second-order effects. For example, the "noise" (i.e., distracting information) created by organizations that implement the cyber resiliency techniques of Diversity, Deception, and Unpredictability can help improve their detection capabilities and potentially reveal the presence of adversaries. Second-order effects are beyond the scope of this publication.

APPENDIX E

CONTROLS SUPPORTING CYBER RESILIENCY

NIST SP 800-53 SECURITY CONTROLS RELATED TO CYBER RESILIENCY

This appendix identifies controls[125] in [SP 800-53] that directly support cyber resiliency. The methodology for determining whether a control directly supports cyber resiliency is outlined below. One of the challenges is that many controls can be considered to provide cybersecurity as well as cyber resiliency. In addition, many security practices that might, in principle, be considered good cybersecurity practices are not widely employed. Therefore, in these cases, if the control satisfies the other screening questions, the control is included in the listing. For each control in [SP 800-53], the following questions were used to identify controls that support cyber resiliency.

- Is the control *primarily* focused on helping the system achieve a level of confidentiality, integrity, or availability[126] in situations where threats, excluding APT, are considered? If so, the control supports conventional information security. The control may provide functional, architectural, governance, or procedural capabilities that establish a necessary foundation for cyber resiliency. However, the control does not support cyber resiliency as a primary consideration.
- Is the control *primarily* focused on ensuring the continuity of operations against threats of natural disasters, infrastructure failures, or cascading failures in which software or human errors are implicated? If so, the control supports *organizational* or *operational resilience* in the face of conventional threats. The control may provide functional, architectural, governance, or procedural capabilities that establish a necessary foundation for cyber resiliency. However, it does not support cyber resiliency, per se.
- Does the control map to one or more of the 14 cyber resiliency techniques? The techniques characterize ways to achieve one or more cyber resiliency objectives. For some controls, mapping to a technique or an approach is trivial. For example, the control SI-14 (Non-Persistence) maps to the cyber resiliency technique of Non-Persistence as the control and cyber resiliency technique share the same name and achieve the same outcome. In other instances, the mapping is relatively straightforward, although not quite as trivial. For example, SC-29 (Heterogeneity) is about the use of diverse information resources so it supports the cyber resiliency Diversity technique. In other instances, the mapping is not as straightforward, and the guidance listed below should be employed to help identify cyber resiliency controls.
- Does the control map to one of the cyber resiliency approaches that support the 14 cyber resiliency techniques? For example, SC-30(4) (Concealment and Misdirection | Misleading Information) maps to the Disinformation approach of the Deception technique. Since the approaches provide a finer granularity than the techniques, this question provides a more

[125] For the remainder of this appendix, the term *control* includes both base controls (e.g., AC-6) and control enhancements (e.g., AC-6(1)).

[126] The control baselines in [SP 800-53B] are defined for levels of concern for confidentiality, integrity, and availability with respect to threats other than the advanced persistent threat.

detailed analysis of the controls, and a control that maps to an approach is *likely* to be a resiliency control.

Many of the controls in [SP 800-53] address other important types of safeguards that are not necessarily related to cyber resiliency. Controls of this type are generally *not* included in the set of controls that support cyber resiliency. These controls include:

- **Policy controls (the -1 controls)**

  The -1 controls (the policy and procedure controls) do not directly map to cyber resiliency techniques or approaches. Only a policy control that is specifically written to address the APT should be identified as a cyber resiliency control.

- **Documentation controls**

  Like the policy controls, documentation controls generally do not satisfy the conditions listed above. A documentation control would have to be narrowly focused (e.g., document how to respond to the presence of the advanced persistent threat) for it to be considered a cyber resiliency control.

- **Environmental controls (e.g., A/C, heating, found in PE family)**

  Environmental controls do not satisfy the conditions listed above unless they are narrowly focused (e.g., controls that address intentional power surges).

- **Personnel security controls**

  Personnel security controls do not satisfy the conditions listed above.

- **Compliance controls (e.g., those checking to ensure that all patches are up to date)**

  Cyber resiliency focuses primarily on evolving and adapting rather than on compliance. Thus, unless a control is explicitly focused on ensuring that some specific (already established) cyber resiliency capability is implemented correctly and operating as intended, compliance controls are generally not considered part of cyber resiliency.

- **Vulnerability assessment controls**

  While adversaries take advantage of vulnerabilities, identifying such vulnerabilities is not the focus of cyber resiliency.

Some control families are more likely to support cyber resiliency than others. The Contingency Planning (CP), Incident Response (IR), System and Communications Protection (SC), and System and Information Integrity (SI) families have a high percentage of controls that are cyber resiliency-oriented. However, controls that support cyber resiliency are not confined to these families, nor are all controls in these families automatically controls supporting cyber resiliency.

After applying the above criteria, there may still be some ambiguity for some controls as to whether or not they are cyber resiliency in their focus. This is due in part to the overlap between aspects of cybersecurity and cyber resiliency. Delineation between the two is not easy to discern. To illustrate the distinction, it is useful to reference first principles.

Cyber resiliency is essentially about ensuring continued mission operations despite the fact that an adversary has established a foothold in the organization's systems and cyber infrastructure.

- Controls that are largely focused on keeping the adversary out of systems and infrastructure are generally not resiliency controls. For example, identification and authentication controls such as IA-4 (Identifier Management) are generally not focused on combating an adversary after they have achieved a foothold in an organizational system. Similarly, physical access controls (e.g., PE-2, PE-4) are generally considered basic information security measures, not cyber resiliency measures.
- One area where there is likely to be some confusion is between Auditing and Analytic Monitoring. Controls that are focused on the correlation of collected information are more likely to be Analytic Monitoring-focused. Controls that are focused on storage capacity for audit trails, what information should be captured in an audit trail, or retention of the audit trail are more likely to fall into the Audit domain.
- In many instances, cyber resiliency capabilities are reflected in control enhancements instead of base controls. In those situations, [SP 800-53] requires that a parent control be selected if one or more of its control enhancements are selected. This means that for any cyber resiliency control enhancement selected, the associated base control is also selected and included in the security plan for the system.

Table E-1 identifies the controls and control enhancements in [SP 800-53] that support cyber resiliency using the criteria outlined above. For each of the selected "cyber resiliency controls or control enhancements," the table specifies the corresponding cyber resiliency technique and approach. In many instances, more than a single cyber resiliency technique or approach is provided because many of the controls and enhancements support more than one cyber resiliency technique or approach. If there are multiple corresponding cyber resiliency techniques, they are listed in a *prioritized* order where the technique with the strongest linkage is listed first. The table will be updated as new versions of [SP 800-53] are published.

TABLE E-1: NIST CONTROLS SUPPORTING CYBER RESILIENCY TECHNIQUES

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]
ACCESS CONTROL		
AC-2(6)	ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT	Privilege Restriction [Dynamic Privileges] Adaptive Response [Dynamic Reconfiguration]
AC-2(8)	ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT MANAGEMENT	Adaptive Response [Dynamic Resource Allocation, Dynamic Reconfiguration, Adaptive Management] Privilege Restriction [Dynamic Privileges]
AC-2(12)	ACCOUNT MANAGEMENT | ACCOUNT MONITORING FOR ATYPICAL USAGE	Analytic Monitoring [Monitoring and Damage Assessment] Substantiated Integrity [Behavior Validation]
AC-3(2)	ACCESS ENFORCEMENT | DUAL AUTHORIZATION	Privilege Restriction [Trust-Based Privilege Management]
AC-3(11)	ACCESS ENFORCEMENT | RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES	Privilege Restriction [Attribute-Based Usage Restriction]
AC-3(12)	ACCESS ENFORCEMENT | ASSERT AND ENFORCE APPLICATION ACCESS	Privilege Restriction [Attribute-Based Usage Restriction]

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]
AC-3(13)	ACCESS ENFORCEMENT | ATTRIBUTE-BASED ACCESS CONTROL	Privilege Restriction [Attribute-Based Usage Restriction]
AC-4(2)	INFORMATION FLOW ENFORCEMENT | PROCESSING DOMAINS	Segmentation [Predefined Segmentation]
AC-4(3)	INFORMATION FLOW ENFORCEMENT | DYNAMIC INFORMATION FLOW CONTROL	Adaptive Response [Dynamic Reconfiguration, Adaptive Management]
AC-4(8)	INFORMATION FLOW ENFORCEMENT | SECURITY AND PRIVACY POLICY FILTERS	Substantiated Integrity [Integrity Checks]
AC-4(12)	INFORMATION FLOW ENFORCEMENT | DATA TYPE IDENTIFIERS	Substantiated Integrity [Integrity Checks]
AC-4(17)	INFORMATION FLOW ENFORCEMENT | DOMAIN AUTHENTICATION	Substantiated Integrity [Provenance Tracking]
AC-4(21)	INFORMATION FLOW ENFORCEMENT | PHYSICAL OR LOGICAL SEPARATION OF INFORMATION FLOWS	Segmentation [Predefined Segmentation]
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 [Attribute-Based Usage Restriction]
AC-6(1)	LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS	Privilege Restriction [Attribute-Based Usage Restriction]
AC-6(2)	LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS	Privilege Restriction [Trust-Based Privilege Management] Realignment [Purposing]
AC-6(3)	LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS	Privilege Restriction [Trust-Based Privilege Management]
AC-6(4)	LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS	Privilege Restriction [Trust-Based Privilege Management, Attribute-Based Usage Restriction] Segmentation [Predefined Segmentation]
AC-6(5)	LEAST PRIVILEGE | PRIVILEGED ACCOUNTS	Privilege Restriction [Trust-Based Privilege Management]
AC-6(6)	LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS	Privilege Restriction [Trust-Based Privilege Management]
AC-6(7)	LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES	Coordinated Protection [Consistency Analysis] Privilege Restriction [Trust-Based Privilege Management]
AC-6(8)	LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION	Privilege Restriction [Attribute-Based Usage Restriction, Dynamic Privileges]

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]
AC-6(10)	LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS	Privilege Restriction [Attribute-Based Usage Restriction, Trust-Based Privilege Management]
AC-7(4)	UNSUCCESSFUL LOGON ATTEMPTS | USE OF ALTERNATE AUTHENTICATION FACTOR	Diversity [Path Diversity]
AC-12	SESSION TERMINATION	Non-Persistence [Non-Persistent Services]
AC-23	DATA MINING PROTECTION	Analytic Monitoring [Monitoring and Damage Assessment] Privilege Restriction [Trust-Based Privilege Management, Attribute-Based Usage Restriction, Dynamic Privileges]
AWARENESS AND TRAINING		
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]
AUDIT AND ACCOUNTABILITY		
AU-5(3)	RESPONSE TO AUDIT PROCESSING FAILURES | CONFIGURABLE TRAFFIC VOLUME THRESHOLDS	Adaptive Response [Dynamic Resource Allocation, Adaptive Management]
AU-6	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING	Adaptive Response [Adaptive Management] Analytic Monitoring [Monitoring and Damage Assessment] Substantiated Integrity [Behavior Validation]
AU-6(3)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES	Analytic Monitoring [Sensor Fusion and Analysis]
AU-6(5)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | INTEGRATED ANALYSIS OF AUDIT RECORDS	Analytic Monitoring [Sensor Fusion and Analysis]
AU-6(6)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING	Analytic Monitoring [Sensor Fusion and Analysis]
AU-6(8)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS	Analytic Monitoring [Monitoring and Damage Assessment] Segmentation [Predefined Segmentation]
AU-6(9)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES	Analytic Monitoring [Sensor Fusion and Analysis]
AU-9(1)	PROTECTION OF AUDIT INFORMATION | HARDWARE WRITE-ONCE MEDIA	Substantiated Integrity [Integrity Checks]

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]
AU-9(2)	PROTECTION OF AUDIT INFORMATION | STORE ON SEPARATE PHYSICAL SYSTEMS AND COMPONENTS	Segmentation [Predefined Segmentation]
AU-9(3)	PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION	Substantiated Integrity [Integrity Checks]
AU-9(5)	PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION	Privilege Restriction [Trust-Based Privilege Management]
AU-9(6)	PROTECTION OF AUDIT INFORMATION | READ-ONLY ACCESS	Privilege Restriction [Trust-Based Privilege Management, Attribute-Based Usage Restriction] Substantiated Integrity [Integrity Checks]
AU-9(7)	PROTECTION OF AUDIT INFORMATION | STORE ON COMPONENT WITH DIFFERENT OPERATING SYSTEM	Diversity [Architectural Diversity]
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]
ASSESSMENT, AUTHORIZATION, AND MONITORING		
CA-7(3)	CONTINUOUS MONITORING | TREND ANALYSES	Contextual Awareness [Dynamic Resource Awareness, Dynamic Threat Awareness]
CA-7(5)	CONTINUOUS MONITORING | CONSISTENCY ANALYSIS	Coordinated Protection [Consistency Analysis]
CA-7(6)	CONTINUOUS MONITORING | AUTOMATION SUPPORT FOR MONITORING	Analytic Monitoring [Monitoring and Damage Assessment]
CA-8	PENETRATION TESTING	Coordinated Protection [Self-Challenge]
CA-8(1)	PENETRATION TESTING | INDEPENDENT PENETRATION TESTING AGENT OR TEAM	Coordinated Protection [Self-Challenge]
CA-8(2)	PENETRATION TESTING | RED TEAM EXERCISES	Coordinated Protection [Self-Challenge]
CA-8(3)	PENETRATION TESTING | FACILITY PENETRATION TESTING	Coordinated Protection [Self-Challenge]
CONFIGURATION MANAGEMENT		
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]
CM-4(1)	IMPACT ANALYSES | SEPARATE TEST ENVIRONMENTS	Segmentation [Predefined Segmentation]
CM-5(3)	ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS	Substantiated Integrity [Integrity Checks, Provenance Tracking]
CM-5(4)	ACCESS RESTRICTIONS FOR CHANGE | DUAL AUTHORIZATION	Privilege Restriction [Trust-Based Privilege Management]
CM-5(5)	ACCESS RESTRICTIONS FOR CHANGE | PRIVILEGE LIMITATION FOR PRODUCTION AND OPERATION	Privilege Restriction [Trust-Based Privilege Management]

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]
CM-5(6)	ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES	Privilege Restriction Trust-Based Privilege Management]
CM-7(2)	LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION	Realignment [Restriction]
CM-7(4)	LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE	Realignment [Purposing]
CM-7(5)	LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE	Privilege Restriction [Trust-Based Privilege Management] Segmentation [Predefined Segmentation, Dynamic Segmentation and Isolation]
CM-7(6)	LEAST FUNCTIONALITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES	Realignment [Purposing]
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]
CM-14	SIGNED COMPONENTS	Substantiated Integrity [Integrity Checks, Provenance Tracking]
CONTINGENCY PLANNING		
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]
CP-2(8)	CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS	Contextual Awareness [Mission Dependency and Status Visualization]
CP-4(5)	SELF-CHALLENGE	Coordinated Protection [Self-Challenge]
CP-8(3)	TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY AND ALTERNATE PROVIDERS	Diversity [Architectural Diversity]
CP-9	SYSTEM BACKUP	Redundancy [Protected Backup and Restore]
CP-9(1)	SYSTEM BACKUP | TESTING FOR RELIABILITY AND INTEGRITY	Redundancy [Protected Backup and Restore] Substantiated Integrity [Integrity Checks]
CP-9(6)	SYSTEM BACKUP | REDUNDANT SECONDARY SYSTEM	Redundancy [Replication]
CP-9(7)	SYSTEM BACKUP | DUAL AUTHORIZATION	Privilege Restriction [Trust-Based Privilege Management]
CP-9(8)	SYSTEM BACKUP | CRYPTOGRAPHIC PROTECTION	Deception [Obfuscation] Redundancy [Protected Backup and Restore] Substantiated Integrity [Integrity Checks]
CP-11	ALTERNATE COMMUNICATIONS PROTOCOLS	Diversity [Architectural Diversity, Design Diversity]
CP-12	SAFE MODE	Adaptive Response [Adaptive Management]
CP-13	ALTERNATIVE SECURITY MECHANISMS	Diversity [Architectural Diversity, Design Diversity] Adaptive Response [Adaptive Management]

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]
IDENTIFICATION AND AUTHENTICATION		
IA-2(6)	IDENTIFICATION AND AUTHENTICATION | ACCESS TO ACCOUNTS – SEPARATE DEVICE	Diversity [Path Diversity] Coordinated Protection [Calibrated Defense-in-Depth, Orchestration]
IA-2(13)	IDENTIFICATION AND AUTHENTICATION | OUT-OF-BAND AUTHENTICATION	Diversity [Path Diversity] Coordinated Protection [Calibrated Defense-in-Depth, Orchestration] Segmentation [Predefined Segmentation]
IA-3(1)	DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION	Deception [Obfuscation] Substantiated Integrity [Integrity Checks]
IA-10	ADAPTIVE AUTHENTICATION	Adaptive Response [Adaptive Management] Privilege Restriction [Dynamic Privileges] Coordinated Protection [Calibrated Defense-in-Depth]
INCIDENT RESPONSE		
IR-4(2)	INCIDENT HANDLING | DYNAMIC RECONFIGURATION	Adaptive Response [Dynamic Reconfiguration] Dynamic Positioning [Functional Relocation of Sensors]
IR-4(3)	INCIDENT HANDLING | CONTINUITY OF OPERATIONS	Adaptive Response [Dynamic Reconfiguration, Adaptive Management] Coordinated Protection [Orchestration]
IR-4(4)	INCIDENT HANDLING | INFORMATION CORRELATION	Coordinated Protection [Orchestration] Analytic Monitoring [Sensor Fusion and Analysis] Contextual Awareness [Dynamic Threat Awareness]
IR-4(9)	INCIDENT HANDLING | DYNAMIC RESPONSE CAPABILITY	Adaptive Response [Dynamic Reconfiguration]
IR-4(10)	INCIDENT HANDLING | SUPPLY CHAIN COORDINATION	Coordinated Protection [Orchestration]
IR-4(11)	INCIDENT HANDLING | INTEGRATED INCIDENT RESPONSE TEAM	Adaptive Response [Dynamic Reconfiguration, Adaptive Management] Analytic Monitoring [Forensic and Behavioral Analysis] Coordinated Protection [Orchestration]
IR-4(12)	INCIDENT HANDLING | MALICIOUS CODE AND FORENSIC ANALYSIS	Analytic Monitoring [Forensic and Behavioral Analysis] Segmentation [Predefined Segmentation]
IR-4(13)	INCIDENT HANDLING | BEHAVIOR ANALYSIS	Analytic Monitoring [Monitoring and Damage Assessment] Substantiated Integrity [Behavior Validation]
IR-5	INCIDENT MONITORING	Analytic Monitoring [Monitoring and Damage Assessment, Forensic and Behavioral Analysis]

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]
MAINTENANCE		
MA-4(4)	NONLOCAL MAINTENANCE | AUTHENTICATION AND SEPARATION OF MAINTENANCE SESSIONS	Segmentation [Predefined Segmentation]
PHYSICAL AND ENVIRONMENTAL PROTECTION		
PE-3(5)	PHYSICAL ACCESS CONTROL | TAMPER PROTECTION	Substantiated Integrity [Integrity Checks]
PE-6	MONITORING PHYSICAL ACCESS	Analytic Monitoring [Monitoring and Damage Assessment]
PE-6(2)	MONITORING PHYSICAL ACCESS | AUTOMATED INTRUSION RECOGNITION AND RESPONSES	Analytic Monitoring [Monitoring and Damage Assessment] Adaptive Response [Adaptive Management] Coordinated Protection [Orchestration]
PE-6(4)	MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO SYSTEMS	Analytic Monitoring [Monitoring and Damage Assessment] Coordinated Protection [Calibrated Defense-in-Depth]
PE-9(1)	POWER EQUIPMENT AND CABLING | REDUNDANT CABLING	Redundancy [Replication]
PE-11(1)	EMERGENCY POWER | ALTERNATE POWER SUPPLY – MINIMAL OPERATIONAL CAPABILITY	Redundancy [Replication]
PE-11(2)	EMERGENCY POWER | ALTERNATE POWER SUPPLY – SELF-CONTAINED	Redundancy [Replication]
PE-17	ALTERNATE WORK SITE	Redundancy [Replication]
PLANNING		
PL-8(1)	SECURITY AND PRIVACY ARCHITECTURE | DEFENSE IN DEPTH	Coordinated Protection [Calibrated]
PL-8(2)	SECURITY AND PRIVACY ARCHITECTURE | SUPPLIER DIVERSITY	Diversity [Supply Chain Diversity]
PROGRAM MANAGEMENT		
PM-7(1)	ENTERPRISE ARCHITECTURE | OFFLOADING	Realignment [Offloading]
PM-16	THREAT AWARENESS PROGRAM	Contextual Awareness [Dynamic Threat Awareness]
PM-16(1)	THREAT AWARENESS PROGRAM | AUTOMATED MEANS FOR SHARING THREAT INTELLIGENCE	Contextual Awareness [Dynamic Threat Awareness]
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]
PM-32	PURPOSING	Realignment [Purposing]
RISK ASSESSMENT		
RA-3(2)	RISK ASSESSMENT | USE OF ALL-SOURCE INTELLIGENCE	Contextual Awareness [Dynamic Threat Awareness]

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]
RA-3(3)	RISK ASSESSMENT | DYNAMIC THREAT AWARENESS	Contextual Awareness [Dynamic Threat Awareness] Adaptive Response [Adaptive Management]
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]
RA-5(6)	VULNERABILITY MONITORING AND SCANNING | AUTOMATED TREND ANALYSES	Analytic Monitoring [Sensor Fusion and Analysis]
RA-5(8)	VULNERABILITY MONITORING AND SCANNING | REVIEW HISTORIC AUDIT LOGS	Analytic Monitoring [Sensor Fusion and Analysis]
RA-5(10)	VULNERABILITY MONITORING AND SCANNING | CORRELATE SCANNING INFORMATION	Analytic Monitoring [Sensor Fusion and Analysis]
RA-9	CRITICALITY ANALYSIS	Contextual Awareness [Mission Dependency and Status Visualization] Realignment [Offloading]
RA-10	THREAT HUNTING	Analytic Monitoring [Monitoring and Damage Assessment] Contextual Awareness [Dynamic Threat Awareness]
SYSTEM AND SERVICES ACQUISITION		
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 [Evolvability, Specialization] Segmentation [Predefined Segmentation]
SA-8(4)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | PARTIALLY ORDERED DEPENDENCIES	Coordinated Protection [Consistency Analysis]
SA-8(6)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | MINIMIZED SHARING	Realignment [Purposing, Restriction] Segmentation [Predefined Segmentation]
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(15)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | PREDICATE PERMISSION	Privilege Restriction [Trust-Based Privilege Management, Attribute-Based Usage Restriction]

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]
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]
SA-11(5)	DEVELOPER TESTING AND EVALUATION | PENETRATION TESTING	Coordinated Protection [Self-Challenge]
SA-11(6)	DEVELOPER TESTING AND EVALUATION | ATTACK SURFACE REVIEWS	Realignment [Replacement]
SA-15(5)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION	Realignment [Replacement]
SA-17(6)	DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR TESTING	Realignment [Evolvability]
SA-17(8)	DEVELOPER SECURITY ARCHITECTURE AND DESIGN | ORCHESTRATION	Coordinated Protection [Orchestration]
SA-17(9)	DEVELOPER SECURITY ARCHITECTURE AND DESIGN | DESIGN DIVERSITY	Diversity [Design Diversity]
SA-20	CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS	Realignment [Specialization]
SA-23	SPECIALIZATION	Realignment [Specialization]
SYSTEM AND COMMUNICATIONS PROTECTION		
SC-2	SEPARATION OF SYSTEM AND USER FUNCTIONALITY	Segmentation [Predefined Segmentation]
SC-2(1)	SEPARATION OF SYSTEM AND USER FUNCTIONALITY | INTERFACES FOR NON-PRIVILEGED USERS	Segmentation [Predefined Segmentation]
SC-3	SECURITY FUNCTION ISOLATION	Segmentation [Predefined Segmentation]
SC-3(1)	SECURITY FUNCTION ISOLATION | HARDWARE SEPARATION	Segmentation [Predefined Segmentation]
SC-3(2)	SECURITY FUNCTION ISOLATION | ACCESS AND FLOW CONTROL FUNCTIONS	Segmentation [Predefined Segmentation]
SC-3(3)	SECURITY FUNCTION ISOLATION | MINIMIZE NONSECURITY FUNCTIONALITY	Realignment [Restriction]

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]
SC-3(5)	SECURITY FUNCTION ISOLATION | LAYERED STRUCTURES	Coordinated Protection [Orchestration] Segmentation [Predefined Segmentation] Realignment [Offloading]
SC-5(2)	DENIAL OF SERVICE PROTECTION | CAPACITY, BANDWIDTH, AND REDUNDANCY	Adaptive Response [Dynamic Resource Allocation] Redundancy [Surplus Capacity]
SC-5(3)	DENIAL OF SERVICE PROTECTION | DETECTION AND MONITORING	Analytic Monitoring [Monitoring and Damage Assessment]
SC-7	BOUNDARY PROTECTION	Segmentation [Predefined Segmentation]
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]
SC-7(11)	BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC	Substantiated Integrity [Provenance Tracking]
SC-7(13)	BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS, MECHANISMS, AND SUPPORT COMPONENTS	Segmentation [Predefined Segmentation]
SC-7(15)	BOUNDARY PROTECTION | NETWORK PRIVILEGE ACCESSES	Realignment [Offloading] Segmentation [Predefined Segmentation] Privilege Restriction [Trust-Based Privileged Management]
SC-7(16)	BOUNDARY PROTECTION | PREVENT DISCOVERY OF SYSTEM COMPONENTS	Deception [Obfuscation] Dynamic Positioning [Functional Relocation of Cyber Resources]
SC-7(20)	BOUNDARY PROTECTION | DYNAMIC ISOLATION AND SEGREGATION	Segmentation [Dynamic Segmentation and Isolation] Adaptive Response [Dynamic Reconfiguration]
SC-7(21)	BOUNDARY PROTECTION | ISOLATION OF SYSTEM COMPONENTS	Segmentation [Predefined Segmentation]
SC-7(22)	BOUNDARY PROTECTION | SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS	Segmentation [Predefined Segmentation]
SC-7(29)	BOUNDARY PROTECTION | SEPARATE SUBNETS TO ISOLATE FUNCTIONS	Segmentation [Predefined Segmentation]
SC-8(1)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION	Substantiated Integrity [Integrity Checks]
SC-8(4)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL OR RANDOMIZE COMMUNICATIONS	Deception [Obfuscation] Unpredictability [Contextual Unpredictability]
SC-8(5)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PROTECTED DISTRIBUTION SYSTEM	Substantiated Integrity [Integrity Checks] Segmentation [Predefined Segmentation]
SC-10	NETWORK DISCONNECT	Non-Persistence [Non-Persistent Connectivity]
SC-11	TRUSTED PATH	Segmentation [Predefined Segmentation] Substantiated Integrity [Provenance Tracking]

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]
SC-15(1)	COLLABORATIVE COMPUTING DEVICES | PHYSICAL OR LOGICAL DISCONNECT	Non-Persistence [Non-Persistent Connectivity]
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]
SC-22	ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE	Redundancy [Replication]
SC-23(3)	SESSION AUTHENTICITY | UNIQUE SYSTEM-GENERATED SESSION IDENTIFIERS	Non-Persistence [Non-Persistent Information] Unpredictability [Temporal Unpredictability]
SC-25	THIN NODES	Realignment [Offloading, Restriction] Non-Persistence [Non-Persistent Services, Non-Persistent Information]
SC-26	DECOYS	Deception [Misdirection] Analytic Monitoring [Monitoring and Damage Assessment, Forensic and Behavioral Analysis]
SC-28(1)	PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION	Deception [Obfuscation] Substantiated Integrity [Integrity Checks]
SC-29	HETEROGENEITY	Diversity [Architectural Diversity]
SC-29(1)	HETEROGENEITY | VIRTUALIZATION TECHNIQUES	Diversity [Architectural Diversity] Non-Persistence [Non-Persistent Services]
SC-30	CONCEALMENT AND MISDIRECTION	Deception [Obfuscation, Misdirection]
SC-30(2)	CONCEALMENT AND MISDIRECTION | RANDOMNESS	Unpredictability [Temporal Unpredictability, Contextual Unpredictability]
SC-30(3)	CONCEALMENT AND MISDIRECTION | CHANGE PROCESSING AND STORAGE LOCATIONS	Dynamic Positioning [Asset Mobility, Functional Relocation of Cyber Resources] Unpredictability [Temporal Unpredictability]
SC-30(4)	CONCEALMENT AND MISDIRECTION | MISLEADING INFORMATION	Deception [Disinformation]
SC-30(5)	CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM COMPONENTS	Deception [Obfuscation]
SC-32	SYSTEM PARTITIONING	Segmentation [Predefined Segmentation]
SC-32(1)	SYSTEM PARTITIONING | SEPARATE PHYSICAL DOMAINS FOR PRIVILEGED FUNCTIONS	Segmentation [Predefined Segmentation, Dynamic Segmentation and Isolation]
SC-34	NON-MODIFIABLE EXECUTABLE PROGRAMS	Substantiated Integrity [Integrity Checks]
SC-34(1)	NON-MODIFIABLE EXECUTABLE PROGRAMS | NO WRITABLE STORAGE	Non-Persistence [Non-Persistent Information]
SC-34(2)	NON-MODIFIABLE EXECUTABLE PROGRAMS | INTEGRITY PROTECTION ON READ-ONLY MEDIA	Substantiated Integrity [Integrity Checks]
SC-35	EXTERNAL MALICIOUS CODE IDENTIFICATION	Analytic Monitoring [Monitoring and Damage Assessment, Forensic and Behavioral Analysis] Deception [Misdirection]

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]
		Segmentation [Dynamic Segmentation and Isolation]
SC-36	DISTRIBUTED PROCESSING AND STORAGE	Dynamic Positioning [Distributed Functionality, Functional Relocation of Cyber Resources] Redundancy [Replication]
SC-36(1)	DISTRIBUTED PROCESSING AND STORAGE | POLLING TECHNIQUES	Substantiated Integrity [Behavior Validation]
SC-36(2)	DISTRIBUTED PROCESSING AND STORAGE | SYNCHRONIZATION	Redundancy [Replication] Coordinated Protection [Orchestration]
SC-37	OUT-OF-BAND CHANNELS	Diversity [Path Diversity]
SC-39	PROCESS ISOLATION	Segmentation [Predefined Segmentation, Dynamic Segmentation and Isolation]
SC-39(1)	PROCESS ISOLATION | HARDWARE SEPARATION	Segmentation [Predefined Segmentation, Dynamic Segmentation and Isolation]
SC-39(2)	PROCESS ISOLATION | SEPARATION EXECUTION DOMAINS PER THREAD	Segmentation [Predefined Segmentation, Dynamic Segmentation and Isolation]
SC-40(2)	WIRELESS LINK PROTECTION | REDUCE DETECTION POTENTIAL	Deception [Obfuscation]
SC-40(3)	WIRELESS LINK PROTECTION | IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION	Deception [Obfuscation] Unpredictability [Temporal Unpredictability, Contextual Unpredictability]
SC-44	DETONATION CHAMBERS	Segmentation [Predefined Segmentation] Analytic Monitoring [Forensic and Behavioral Analysis] Deception [Misdirection]
SC-46	CROSS-DOMAIN POLICY ENFORCEMENT	Segmentation [Predefined Segmentation]
SC-47	ALTERNATE COMMUNICATION PATHS	Diversity [Path Diversity]
SC-48	SENSOR RELOCATION	Dynamic Positioning [Functional Relocation of Sensors]
SC-48(1)	SENSOR RELOCATION | DYNAMIC RELOCATION OF SENSORS OR MONITORING CAPABILITIES	Dynamic Positioning [Functional Relocation of Sensors]
SC-49	HARDWARE-ENFORCED SEPARATION AND POLICY ENFORCEMENT	Segmentation [Predefined Segmentation]
SC-50	SOFTWARE-ENFORCED SEPARATION AND POLICY ENFORCEMENT	Segmentation [Predefined Segmentation]
SC-51	NON-MODIFIABLE EXECUTABLE PROGRAMS | HARDWARE-BASED PROTECTION	Substantiated Integrity [Integrity Checks]
SYSTEM AND INFORMATION INTEGRITY		
SI-3(10)	MALICIOUS CODE PROTECTION | MALICIOUS CODE ANALYSIS	Analytic Monitoring [Forensic and Behavioral Analysis]
SI-4(1)	SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM	Analytic Monitoring [Sensor Fusion and Analysis] Contextual Awareness [Mission Dependency and Status Visualization]

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]
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]
SI-4(3)	SYSTEM MONITORING | AUTOMATED TOOL AND MECHANISM INTEGRATION	Analytic Monitoring [Sensor Fusion and Analysis] Adaptive Response [Adaptive Management]
SI-4(4)	SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC	Analytic Monitoring [Monitoring and Damage Assessment] Substantiated Integrity [Behavior Validation]
SI-4(7)	SYSTEM MONITORING | AUTOMATED RESPONSE TO SUSPICIOUS EVENTS	Analytic Monitoring [Monitoring and Damage Assessment] Adaptive Response [Adaptive Management]
SI-4(10)	SYSTEM MONITORING | VISIBILITY OF ENCRYPTED COMMUNICATIONS	Analytic Monitoring [Monitoring and Damage Assessment]
SI-4(11)	SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES	Analytic Monitoring [Monitoring and Damage Assessment]
SI-4(13)	SYSTEM MONITORING | ANALYZE TRAFFIC AND EVENT PATTERNS	Analytic Monitoring [Monitoring and Damage Assessment] Substantiated Integrity [Behavior Validation]
SI-4(16)	SYSTEM MONITORING | CORRELATE MONITORING INFORMATION	Analytic Monitoring [Sensor Fusion and Analysis] Contextual Awareness [Dynamic Resource Awareness]
SI-4(17)	SYSTEM MONITORING | INTEGRATED SITUATIONAL AWARENESS	Analytic Monitoring [Sensor Fusion and Analysis] Contextual Awareness [Dynamic Resource Awareness]
SI-4(18)	SYSTEM MONITORING | ANALYZE TRAFFIC AND COVERT EXFILTRATION	Analytic Monitoring [Monitoring and Damage Assessment]
SI-4(24)	SYSTEM MONITORING | INDICATORS OF COMPROMISE	Analytic Monitoring [Monitoring and Damage Assessment, Sensor Fusion and Analysis]
SI-4(25)	SYSTEM MONITORING | OPTIMIZE NETWORK TRAFFIC ANALYSIS	Analytic Monitoring [Sensor Fusion and Analysis]
SI-6	SECURITY AND PRIVACY FUNCTION VERIFICATION	Substantiated Integrity [Integrity Checks]
SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	Substantiated Integrity [Integrity Checks]
SI-7(1)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS	Substantiated Integrity [Integrity Checks]
SI-7(5)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS	Substantiated Integrity [Integrity Checks] Adaptive Response [Adaptive Management]
SI-7(6)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION	Substantiated Integrity [Integrity Checks]

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]
SI-7(7)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE	Substantiated Integrity [Integrity Checks] Analytic Monitoring [Monitoring and Damage Assessment]
SI-7(9)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | VERIFY BOOT PROCESS	Substantiated Integrity [Integrity Checks]
SI-7(10)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | PROTECTION OF BOOT FIRMWARE	Substantiated Integrity [Integrity Checks]
SI-7(12)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY VERIFICATION	Substantiated Integrity [Integrity Checks]
SI-7(15)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION	Substantiated Integrity [Provenance Tracking]
SI-10(3)	INFORMATION INPUT VALIDATION |PREDICTABLE BEHAVIOR	Substantiated Integrity [Behavior Validation]
SI-10(5)	INFORMATION INPUT VALIDATION | RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS	Substantiated Integrity [Provenance Tracking]
SI-14	NON-PERSISTENCE	Non-Persistence [Non-Persistent Services]
SI-14(1)	NON-PERSISTENCE | REFRESH FROM TRUSTED SOURCES	Non-Persistence [Non-Persistent Services, Non-Persistent Information] Substantiated Integrity [Provenance Tracking]
SI-14(2)	NON-PERSISTENCE | NON-PERSISTENT INFORMATION	Non-Persistence [Non-Persistent Information]
SI-14(3)	NON-PERSISTENCE | NON-PERSISTENT CONNECTIVITY	Non-Persistence [Non-Persistent Connectivity]
SI-15	INFORMATION OUTPUT FILTERING	Substantiated Integrity [Integrity Checks]
SI-16	MEMORY PROTECTION	Diversity [Synthetic Diversity] Unpredictability [Temporal Unpredictability]
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]
SI-22	INFORMATION DIVERSITY	Diversity [Information Diversity]
SI-23	INFORMATION FRAGMENTATION	Dynamic Positioning [Fragmentation]
SUPPLY CHAIN RISK MANAGEMENT		
SR-3(1)	SUPPLY CHAIN CONTROLS AND PROCESSES | DIVERSE SUPPLY CHAIN	Diversity [Supply Chain Diversity]
SR-3(2)	SUPPLY CHAIN CONTROLS AND PROCESSES | LIMITATION OF HARM	Diversity [Supply Chain Diversity] Deception [Obfuscation]
SR-4	PROVENANCE	Substantiated Integrity [Provenance Tracking]

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]
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]
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]
SR-5(1)	ACQUISITION STRATEGIES, TOOLS, AND METHODS | ADEQUATE SUPPLY	Redundancy [Replication] Diversity [Supply Chain Diversity]
SR-6(1)	SUPPLIER ASSESSMENTS AND REVIEWS | TESTING AND ANALYSIS	Coordinated Protection [Self-Challenge] Analytic Monitoring [Monitoring and Damage Assessment]
SR-7	SUPPLY CHAIN OPERATIONS SECURITY	Deception [Obfuscation, Disinformation, Self-Challenge]
SR-9	TAMPER RESISTANCE AND DETECTION	Substantiated Integrity [Integrity Checks]
SR-9(1)	TAMPER RESISTANCE AND DETECTION | MULTIPLE STAGES OF SYSTEM DEVELOPMENT LIFE CYCLE	Substantiated Integrity [Integrity Checks] Deception [Obfuscation]
SR-10	INSPECTION OF SYSTEMS OR COMPONENTS	Substantiated Integrity [Integrity Checks] Analytic Monitoring [Monitoring and Damage Assessment, Forensic and Behavioral Analysis]
SR-11	COMPONENT AUTHENTICITY	Substantiated Integrity [Integrity Checks, Provenance Tracking]
SR-11(3)	COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT SCANNING	Substantiated Integrity [Integrity Checks]

2946

APPENDIX F

ADVERSARY-ORIENTED ANALYSIS

APPROACHES FOR TAKING ADVERSARIAL ACTIVITIES INTO CONSIDERATION

This appendix supports an adversary-oriented analysis of a system and applications of cyber resiliency, as discussed in Section 3.1.7, Section 3.2.3.2, and Section 3.2.4.3. Section F.1 provides a vocabulary to describe the current or potential effects that a set of mitigations (i.e., risk-reducing actions or decisions, such as the application of cyber resiliency design principles, techniques, implementation approaches, requirements, controls, technologies, or solutions) could have on threat events, classes of threat events, or threat scenarios.[127] Each intended effect is characterized in terms of its potential impact on risk and the expected changes in adversary behavior. Section F.2 presents the results of an analysis of the potential effects of mitigations that apply cyber resiliency approaches and controls on adversary TTPs using ATT&CK® for Enterprise.

F.1 POTENTIAL EFFECTS ON THREAT EVENTS

Cyber resiliency solutions are relevant only if they have some effect on risk, specifically by reducing the likelihood of the occurrence of threat events,[128] the ability of threat events to cause harm, and the extent of that harm.[129] The types of analysis of system architectures, designs, implementations, and operations that are indicated for cyber resiliency can include consideration of what effects alternatives could have on the threat events that are part of threat scenarios of concern to stakeholders.

From the perspective of protecting a system against adversarial threats, five high-level, desired effects on the adversary can be identified: *redirect*, *preclude*, *impede*, *limit*, and *expose*. These effects are useful for discussion but are often too general to facilitate the definition of specific measures of effectiveness. Therefore, more specific classes of effects are defined:

- Deter, divert, and deceive in support of **redirect**
- Expunge, preempt, and negate in support of **preclude**
- Contain, degrade, delay, and exert in support of **impede**
- Shorten and reduce in support of **limit**
- Detect, reveal, and scrutinize in support of **expose**

[127] While this appendix focuses on potential effects on adversary actions, most of the vocabulary applies to threat events caused by the full range of possible threat sources identified in [SP 800-30].

[128] The term *threat event* refers to an event or situation that has the potential to cause undesirable consequences or impacts. Threat events can be caused by either adversarial or non-adversarial threat sources. However, the emphasis in this section is on the effect on adversarial threats and, specifically, on the APT for which threat events can be identified with adversary activities.

[129] While many risk models are potentially valid and useful, three elements (or risk factors) are common across most models: (1) the *likelihood of occurrence* (i.e., the likelihood that a threat event or a threat scenario consisting of a set of interdependent events will occur or be initiated by an adversary), (2) the *likelihood of impact* (i.e., the likelihood that a threat event or scenario will result in an impact given vulnerabilities, weaknesses, and predisposing conditions), and (3) the *level of the impact* [SP 800-30]. In general use, "mitigation" relates to impact reduction. However, when applied to a threat event, mitigation can relate to the reduction of any of these risk factors.

These effects are tactical (i.e., local to a specific threat event or scenario), although it is possible that their repeated achievement could have strategic effects as well. All effects except deter, deceive, and exert apply to non-adversarial and adversarial threat events; deter, deceive, and exert are applicable only to adversarial threat events.

Table F-1 defines the effects and provides informal notes in *italics*. It also indicates how each effect could reduce risk and illustrates how the use of certain approaches to implementing cyber resiliency techniques for protection against attack could have the identified effect. The term *defender* refers to the organization or organizational personnel responsible for providing or applying protections. It should be noted that likelihoods and impact can be reduced, but risk cannot be eliminated. Thus, no effect can be assumed to be complete, even those with names that suggest completeness, such as negate, detect, or expunge. Table F-2 shows the potential effects of cyber resiliency techniques on risk factors.

TABLE F-1: EFFECTS OF CYBER RESILIENCY TECHNIQUES ON ADVERSARIAL THREAT EVENTS

INTENDED EFFECT	IMPACT ON RISK	EXPECTED RESULTS
REDIRECT (includes deter, divert, and deceive) Direct the threat event away from defender-chosen resources.	Reduce the likelihood of occurrence, and (to a lesser extent) reduce the likelihood of impact.	• The adversary's efforts cease. • The adversary actions are mistargeted or misinformed.
DETER Discourage the adversary from taking an action by instilling fear (e.g., of attribution or retribution) or doubt that the action would achieve intended effects (e.g., that targets exist). *This effect is relevant only to adversarial threat events and involves influencing the adversary's decision-making process.*	Reduce the likelihood of occurrence.	• The adversary ceases or suspends activities. **Example:** The defender uses disinformation to make it appear that the organization is better able to detect attacks than it is and is willing to launch major counter-strikes. Therefore, the adversary chooses to not launch an attack due to fear of detection and reprisal.
DIVERT Direct the threat event toward defender-chosen resources. *The event affects resources that the defender does not care about or for which the defender can manage consequences.*	Reduce the likelihood of occurrence.	• The adversary refocuses activities on defender-chosen resources. • The adversary directs activities toward targets beyond the defender's purview (e.g., other organizations). • The adversary does not affect resources that the defender has not selected to be targets. **Example:** The defender maintains an Internet-visible enclave with which untrusted external entities can interact and a private enclave accessible only via a VPN for trusted suppliers, partners, or customers (predefined segmentation). **Example:** The defender uses non-persistent information and obfuscation to hide critical resources combined with functional relocation of cyber resources and disinformation to lure the adversary toward a sandboxed

INTENDED EFFECT	IMPACT ON RISK	EXPECTED RESULTS
		enclave where adversary actions cannot harm critical resources.
DECEIVE Lead the adversary to believe false information about individuals, systems, missions, organizations, defender capabilities, or TTPs. *This effect is relevant only to adversarial threat events and involves influencing the adversary's actions.*	Reduce the likelihood of occurrence, and/or reduce the likelihood of impact.	• The adversary's efforts are wasted as the assumptions on which the adversary bases attacks are false. • The adversary takes actions based on false information, thus revealing that they have obtained that information. **Example:** The defender strategically places false information (disinformation) about the cybersecurity investments that it plans to make. As a result, the adversary's malware development is wasted by being focused on countering non-existent cybersecurity protections. **Example:** The defender uses selectively planted false information (disinformation) and honeynets (misdirection) to cause an adversary to focus its malware on virtual sandboxes while simultaneously employing obfuscation to hide the actual resources.
PRECLUDE (includes expunge, preempt, and negate) Ensure that the threat event does not have an impact.	Reduce the likelihood of occurrence, and/or reduce the likelihood of impact.	• The adversary's efforts or resources cannot be applied or are wasted.
EXPUNGE Remove resources that are known to be or suspected of being unsafe, incorrect, or corrupted.	Reduce the likelihood of impact of subsequent events in the same threat scenario.	• A malfunctioning, misbehaving, or suspect resource is restored to normal operation. • The adversary loses a capability for some period, as adversary-directed threat mechanisms (e.g., malicious code) are removed. • Adversary-controlled resources are so badly damaged that they cannot perform any function or be restored to a usable condition without being entirely rebuilt. **Example:** The defender uses virtualization to refresh critical software (non-persistent services) from a known good copy at random intervals (temporal unpredictability). As a result, malware that was implanted in the software is deleted.
PREEMPT Forestall or avoid conditions under which the threat event could occur. *The threat event cannot have any consequences because it cannot actually occur.*	Reduce the likelihood of occurrence.	• The adversary's resources cannot be applied, or the adversary cannot perform activities (e.g., because resources adversary requires are destroyed or made inaccessible). **Example:** An unneeded network connection is disabled (non-persistent connectivity) so that an attack via that interface cannot be made. **Example:** A resource is repositioned (asset mobility) so that it cannot be affected by a threat event in its new location.
NEGATE Create conditions under which the threat event cannot be expected to result in an impact.	Reduce the likelihood of impact.	• The adversary can launch an attack, but it will not even partially succeed. The adversary's efforts are wasted as the assumptions on which the adversary based its attack are no longer valid, and as a result, the intended effects cannot be achieved.

INTENDED EFFECT	IMPACT ON RISK	EXPECTED RESULTS
The threat event may produce consequences, but those consequences cannot produce an impact.		**Example:** Subtle variations in critical software are implemented (synthetic diversity) and prevent the adversary's malware from compromising the targeted software.
IMPEDE (includes contain, degrade, delay, and exert) Make it more difficult for the threat event to cause adverse impacts or consequences. *For adversarial threats, this involves decreasing the adversary's return on investment (ROI) for the threat event.*	Reduce the likelihood of impact, and reduce the level of impact.	• Adversary activities are restricted in scope, fail to achieve full effect, do not take place in accordance with the adversary timeline, or require greater resources than the adversary had planned.
CONTAIN Restrict the effects of the threat event to a limited set of resources. *The consequences of the threat event are less extensive than they might otherwise be.*	Reduce the level of impact.	• The adversary can affect fewer resources than planned. The value of the activity to the adversary, in terms of achieving the adversary's goals, is reduced. **Example:** The defender organization makes changes to a combination of internal firewalls and logically separated networks (dynamic segmentation) to isolate enclaves in response to the detection of malware, limiting the effects of the malware to initially infected enclaves.
DEGRADE Decrease the expected consequences of the threat event. *Because the consequences of the threat event are less severe than they would be without the mitigation, they could fail to produce an impact, or their impact could be lessened.*	Reduce the likelihood of impact, and/or reduce the level of impact.	• Not all of the resources targeted by the adversary are affected, or the targeted resources are affected to a lesser degree than the adversary sought. **Example:** The defender uses multiple browsers and operating systems (architectural diversity) on both end-user systems and some critical servers. The result is that malware targeted at specific software can only compromise a subset of the targeted systems; a sufficient number continue to operate to complete the mission or business function.
DELAY Increase the amount of time needed for the threat event to result in adverse impacts. *Because the consequences of the threat event occur later than they would without the mitigation, they could fail to produce an impact, or their impact could be lessened.*	Reduce the likelihood of impact, and/or reduce the level of impact.	• The adversary achieves the intended effects but not within the intended period. **Example:** The protection measures (e.g., access controls, encryption) allocated to resources increase in number and strength based on resource criticality (calibrated defense-in-depth). The frequency of authentication challenges varies randomly (temporal unpredictability) and more often for more critical resources. The result is that it takes the attacker more time to successfully compromise the targeted resources.
EXERT Increase the level of effort or resources needed for an adversary to achieve a given result. *This effect is relevant only to adversarial threat events*	Reduce the likelihood of impact.	• The adversary gives up planned or partially completed activities in response to finding that additional effort or resources are needed. • The adversary achieves the intended effects in their desired time frame but only by applying more resources. Thus, the adversary's return on investment (ROI) is decreased.

INTENDED EFFECT	IMPACT ON RISK	EXPECTED RESULTS
and involves increasing the adversary's costs.		• The adversary reveals TTPs they had planned to reserve for future use. **Example:** The defender enhances the defenses of moderate-criticality components with additional mitigations (calibrated defense-in-depth). To overcome these, the adversary must tailor and deploy TTPs that they were planning to reserve for use against higher value defender targets. **Example:** The defender adds a large amount of valid but useless information to a data store (obfuscation), requiring the adversary to exfiltrate and analyze more data before taking further actions.
LIMIT (includes shorten and reduce) Restrict the impacts of a realized threat event by limiting the damage or effects it causes in terms of time, system resources, and/or mission or business impacts.	Reduce the level of impact, and reduce the likelihood of impact of subsequent events in the same threat scenario.	• The adversary's effectiveness is restricted.
SHORTEN Limit the duration of adverse consequences of a threat event. *Because the consequences of the threat event do not persist as long as they would without the mitigation, they could fail to produce an impact, or their impact could be lessened.*	Reduce the level of impact.	• The time period during which the adversary's activities affect defender resources is limited. **Example:** The defender employs a diverse set of suppliers (supply chain diversity) for time-critical components. As a result, when an adversary's attack on one supplier causes it to shut down, the defender can increase its use of the other suppliers, thus shortening the time during which it is without the critical components.
REDUCE Decrease the degree of damage from a threat event. The degree of damage can have two dimensions: breadth (i.e., number of affected resources) and depth (i.e., level of harm to a given resource). *A decrease in the degree of damage lessens the impact.*	Reduce the level of impact.	• The level of damage to organizational missions or business operations from adversary activities is reduced due to partial restoration or reconstitution of all affected resources. **Example:** Resources determined to be corrupted or suspect (integrity checks, behavior validation) are restored from older, uncorrupted resources (protected backup and restore) with reduced functionality. • The level of damage to organizational missions or business operations from adversary activities is reduced due to full restoration or reconstitution of some of the affected resources. **Example:** The organization removes one of three compromised resources and provides a new resource (replacement, specialization) for the same or equivalent mission or business functionality.
EXPOSE (includes detect, scrutinize, and reveal) Reduce risk due to ignorance of threat events	Reduce the likelihood of impact.	• The adversary loses the advantage of stealth as defenders are better prepared by developing and sharing threat intelligence.

INTENDED EFFECT	IMPACT ON RISK	EXPECTED RESULTS
and possible replicated or similar threat events in the same or similar environments.		
DETECT Identify a threat event or its effects by discovering or discerning the fact that the event is occurring, has occurred, or (based on indicators, warnings, and precursor activities) is about to occur. *Detection informs corrective actions.*	Reduce the likelihood of impact, and reduce the level of impact (depending on responses).	• The adversary's activities become susceptible to defensive responses. **Example:** The defender continually moves its sensors (functional relocation of sensors), often at random times (temporal unpredictability), to common points of egress from the organization. They combine this with the use of beacon traps (tainting). The result is that the defender can quickly detect efforts by the adversary to exfiltrate sensitive information.
SCRUTINIZE Analyze threat events and artifacts associated with threat events to develop indicators, assess damage, and identify patterns of exploiting vulnerabilities, predisposing conditions, and weaknesses. *Scrutiny informs more effective detection and risk response.*	Reduce the likelihood of impact.	• The adversary loses the advantages of uncertainty, confusion, and doubt. • The defender has a better understanding the adversary, based on an analysis of the adversary's activities, including the artifacts (e.g., malicious code) and effects associated with those activities and the correlation of activity-specific observations with other activities (as feasible), and thus can recognize adversary TTPs. **Example:** The defender deploys honeynets (misdirection), inviting attacks by the adversary and allowing the adversary to apply its TTPs in a safe environment. The defender then analyzes (malware and forensic analysis) the malware captured in the honeynet to determine the nature of the attacker's TTPs, allowing it to develop appropriate defenses.
REVEAL Share information about risk factors and the relative effectiveness of remediation approaches with partners, stakeholder community, or the general public. *Threat information sharing supports common, joint, or coordinated risk responses. Information about threat events can be shared broadly or with a limited set of threat intelligence information-sharing partners.*	Reduce the likelihood of impact, particularly in the future.	• The adversary loses the advantage of surprise and plausible deniability. • The adversary's ability to compromise one organization's systems to attack another organization is impaired as awareness of adversary characteristics and behavior across the stakeholder community (e.g., across all computer security incident response teams that support a given sector that might be expected to be attacked by the same actor or actors) is increased. **Example:** The defender participates in threat information sharing and uses dynamically updated threat intelligence data feeds (dynamic threat modeling) to inform actions (adaptive management).

2989

2990

2991 **TABLE F-2: EFFECTS OF CYBER RESILIENCY TECHNIQUES ON RISK FACTORS**

	REDUCE IMPACT	REDUCE LIKELIHOOD OF IMPACT	REDUCE LIKELIHOOD OF OCCURENCE
ADAPTIVE RESPONSE	X	X	
ANALYTIC MONITORING		X	
CONTEXTUAL AWARENESS	X	X	
COORDINATED PROTECTION	X	X	
DECEPTION		X	X
DIVERSITY	X	X	
DYNAMIC POSITIONING	X	X	X
NON-PERSISTENCE	X	X	X
PRIVILEGE RESTRICTION	X	X	
REALIGNMENT	X	X	X
REDUNDANCY	X	X	
SEGMENTATION	X	X	
SUBSTANTIATED INTEGRITY	X	X	
UNPREDICTABILITY	X	X	

2992

2993 F.2 ANALYSIS OF POTENTIAL EFFECTS OF CYBER RESILIENCY

2994 The focus of cyber resiliency is on mitigating attacks on systems and organizations from the APT.
2995 It is important to understand what effects these mitigations have on adversaries. Mapping the
2996 current or potential effects of mitigations to a threat taxonomy provides a structured way to
2997 facilitate this understanding. This appendix presents the results of such analysis using ATT&CK
2998 for Enterprise [MITRE18].

2999 ATT&CK provides a knowledge base of adversary tactics, techniques, and associated information
3000 based on curated data sets of real-world observations. ATT&CK reflects the phases of an
3001 adversary's attack lifecycle and the platforms (e.g., Windows) adversaries are known to target,
3002 providing a taxonomy of adversarial TTPs with a focus on those used by external adversaries
3003 executing cyber attacks against networked systems. For purposes of this analysis, the following
3004 components of ATT&CK are relevant:

3005 • Tactics, denoting short-term, tactical adversary goals during an attack

3006 • Techniques, describing the means by which adversaries achieve tactical goals, and given
3007 identifiers of the form T####

3008 • Detection methods for each technique, captured as descriptive text in ATT&CK

- Mitigations, describing technologies and practices which have been observed (in one or more of the curated data sets) to mitigate the techniques with which they are associated, and given identifiers of the form M####

ATT&CK also defines sub-techniques, describing more specific means by which adversaries achieve tactical goals at a lower level than techniques (typically related to specific technologies or platforms), and associates mitigations and detection methods with sub-techniques. ATT&CK provides information about APT groups and about malware used by one or more APT actors. However, the analysis presented below does not consider sub-techniques, groups, malware, or other information included in ATT&CK.

F.2.1. Assumptions and Caveats

The analysis is restricted to mitigations that apply one or more cyber resiliency approaches and use one or more cyber resiliency controls,[130] as identified in Table E-1 and in the ATT&CK knowledge base from curated datasets of real-world data and assigned identifiers of the form M10##. The analysis also uses candidate mitigations[131] defined by engineering analysis but not part of the ATT&CK knowledge base. Candidate mitigations are discussed in Section F.2.4, presented in Tables F-17 through F-19, and assigned identifiers of the form CM11##, CM13##, and CM20##. The analysis excludes from consideration those ATT&CK mitigations that do not apply a cyber resiliency approach but instead use conventional security methods to mitigate the ATT&CK technique. The analysis is restricted to ATT&CK techniques and does not include ATT&CK sub-techniques.

The analysis considers only the direct effects that a particular control could have when implemented and used as described in the context of the mitigation or candidate mitigation. Indirect effects are not identified. Therefore, this analysis does not consider related controls (i.e., base controls for identified cyber resiliency control enhancements, controls identified as related for cyber resiliency controls). Similarly, this analysis does not map controls that influence the system architecture (e.g., control enhancements to SA-8, Security and Privacy Engineering Principles).

Some cyber resiliency controls do not appear in Tables F-3 through F-16. There are two reasons for a control not being referenced in the ATT&CK mapping. First, a control could be intended to address threats not represented in ATT&CK for Enterprise (e.g., insider threats, threats against ICS, threats from maintenance staff, attacks on wireless communications). Second, a control could have no effect on any specific adversary TTP, either directly or by intensifying the effectiveness of an existing mitigation or candidate mitigation. This is particularly the case for design principles and requirements on system development. The effects of these controls are inherently indirect.

Note that this analysis simply *identifies* the potential effects of the implementation approaches. It does not and cannot assess how strongly any identified effect will be experienced by an APT

[130] For brevity, the term *control* will be used to include control enhancements (e.g., AC-6(1)) as well as base controls (e.g., AC-6).

[131] A candidate mitigation is a mitigation, defined in the context of ATT&CK, which has not been derived from a curated data set. It is designated as a "candidate" to differentiate it from the mitigations in the ATT&CK knowledge base.

actor.[132] A more detailed analysis would require knowledge of the type of system (including the system architecture and the types of technologies used) and the organization to which the requirements are to be applied. In addition, more detailed analysis could go beyond mapping to adversary objectives and map to adversary actions or individual adversary TTPs (e.g., as defined by the ATT&CK framework). Finally, some effects are beyond what can be designed and implemented in a technical system or the system's supporting processes and practices. For example, the detection of adversary Resource Development actions requires cyber and other types of intelligence gathering and analyses, which are beyond the scope of cyber resiliency. Similarly, the Reveal effect involves the use of cyber threat intelligence by other organizations.

F.2.2 Potential Uses of Analysis

By seeing which effects a given approach could potentially have on a threat event, the systems engineer can determine which approaches (and corresponding controls) could maximize the system's chances of mitigating the adversary's actions. Thus, using the tables of this appendix may reveal to a systems engineer that the approaches (and correspondingly, the controls) that they are planning to invest in are largely focused on detecting an adversary, containing an adversary's assault, shortening the duration of a successful adversary attack, and reducing the damage from such an attack. Correspondingly, such an assessment would reveal to the system engineer that the organization's planned investments may be lacking in controls that have other effects, such as diverting or deceiving the adversary or preempting or negating the adversary's attempted attack. Such information can help the engineer and other stakeholders reconsider their cyber security investments so that they might be more balanced.

The tables also reveal which approaches (and correspondingly, which controls) have multiple potential effects on the adversary and which have only a few potential effects on the adversary. Such information might help inform investment decisions by guiding stakeholders to controls that have multiple effects, including those in which the organization has not previously invested.

A control or a cyber resiliency approach per se will not have an effect on an adversary TTP—effects are achieved by threat-aware implementation and use of controls and approaches. The descriptions of the candidate mitigations in Section F.2.4 and [Bodeau21] indicate how the implementation and use of controls could have the identified effects. The descriptions of candidate mitigations, which are at a higher level of abstraction than cyber resiliency controls and approaches, and often involve multiple controls and approaches, could also serve as the starting points for system requirements.

Note that not all adversary tactics are affected by all approaches. Some tactics are affected only by one or two approaches. This is generally the case for adversary tactics in the early stages (e.g., Reconnaissance, Resource Development), which largely involve adversary actions done prior to accessing a defender's system.

F.2.3 Results of Analysis

Tables F-3 through F-16 present the results of the analysis of potential effects of cyber resiliency on ATT&CK techniques. For each ATT&CK technique, the analysis includes relevant mitigations

[132] Any true measure of effectiveness will need to be defined and evaluated in a situated manner (i.e., by identifying assumptions about the architectural, technical, operational, and threat environments, as discussed in Section 3.2.1).

or candidate mitigations,[133] cyber resiliency implementation approaches, the potential effects on the adversary when the approaches are applied, and the controls that can be employed to achieve the intended effects.

TABLE F-3: POTENTIAL EFFECTS OF CYBER RESILIENCY ON RECONNAISSANCE TECHNIQUES

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Active Scanning (T1595)	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Passive Decoys (CM1104)	Misdirection	Divert, Deceive	SC-26
		Architectural Diversity	Divert, Exert	SC-29
	Conceal Resources from Discovery (CM1160)	Obfuscation, Functional Relocation of Cyber Resources	Degrade, Exert, Shorten	SC-7(16)
		Obfuscation	Degrade, Exert	SC-28(1), SC-30, SC-30(5)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Gather Victim Host Information (T1592)	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
	Passive Decoys (CM1104)	Misdirection	Divert, Deceive	SC-26
		Architectural Diversity	Divert, Exert	SC-29
	Present Decoy Data (CM1113)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
Gather Victim Identity Information (T1589)	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Present Decoy Data (CM1113)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Enhance User Preparedness (CM1159)	Dynamic Threat Awareness	Exert	AT-2(1), AT-2(5)
		Self-Challenge	Exert	AT-2(1), AT-3(3)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Gather Victim Network Information (T1590)	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26

[133] The purpose of defining *candidate mitigations* is to ensure that the analysis uses a consistent method to identify which cyber resiliency approaches and controls could affect a given ATT&CK technique and to capture the reasoning about how cyber resiliency effects could be achieved. In contrast to the mitigations of ATT&CK, which are derived from operational experience and curated data sets, candidate mitigations are based on engineering analysis.

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Misdirection	Deceive	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Present Decoy Data (CM1113)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Gather Victim Org Information (T1591)	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Present Decoy Data (CM1113)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
Phishing for Information (T1598)	User Training (M1017)	Dynamic Threat Awareness	Preempt, Exert, Detect	AT-2(5)
	Adversarial Simulation (CM1107)	Dynamic Threat Awareness, Self-Challenge	Preempt	AT-2(1), AT-3(3)
	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
	Active Decoys (CM1123)	Misdirection, Forensic and Behavioral Analysis	Detect	SC-35
	Enhance User Preparedness (CM1159)	Dynamic Threat Awareness	Detect	AT-2(1), AT-2(3), AT-2(5), AT-3(3)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	SI-4(13)
Search Closed Sources (T1597)	Adversarial Simulation (CM1107)	Self-Challenge	Detect	CA-8, CA-8(2)
	Collaborate to Counter Adversaries (CM1161)	Disinformation, Tainting	Deceive, Detect	SC-30(4), SI-20
		Dynamic Threat Awareness	Detect	PM-16
	Restrict Supply Chain Exposures (CM1162)	Obfuscation, Supply Chain Diversity	Exert	SR-3(2)
		Disinformation	Deceive	SR-7
		Self-Challenge	Detect	SR-6(1), SR-7
Search Open Technical	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Databases (T1596)	Adversarial Simulation (CM1107)	Self-Challenge	Detect	CA-8, CA-8(2)
	Restrict Supply Chain Exposures (CM1162)	Obfuscation, Supply Chain Diversity	Exert	SR-3(2)
		Disinformation	Deceive	SR-7
		Self-Challenge	Detect	SR-6(1), SR-7
Search Open Websites or Domains (T1593)	Present Decoy Data (CM1113)	Disinformation,	Deceive	SC-30(4)
		Tainting	Detect	SI-20
Search Victim-Owned Websites (T1594)	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Present Decoy Data (CM1113)	Disinformation	Deceive	SC-30(4)

TABLE F-4: POTENTIAL EFFECTS OF CYBER RESILIENCY ON RESOURCE DEVELOPMENT TECHNIQUES

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Acquire Infrastructure (T1583)	Present Deceptive Information (CM1101)	Disinformation	Preempt, Detect	SC-30(4)
	Adversarial Simulation (CM1107)	Self-Challenge	Detect	CA-8, CA-8(2)
	Collaborate to Counter Adversaries (CM1161)	Dynamic Threat Awareness	Detect	PM-16
Compromise Accounts (T1586)	Enhance User Preparedness (CM1159)	Dynamic Threat Awareness	Detect	AT-2(1), AT-2(3), AT-2(5), AT-3(3)
	Monitor External Sources (CM2043)	Monitoring and Damage Assessment, Dynamic Threat Awareness	Detect	AU-13, AU-13(3), RA-5(4), RA-10
Compromise Infrastructure (T1584)	Monitor External Sources (CM2043)	Monitoring and Damage Assessment, Dynamic Threat Awareness	Detect, Scrutinize, Reveal	AU-13, AU-13(3), PM-16, RA-5(4), RA-10

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Develop Capabilities (T1587)	Monitor External Sources (CM2043)	Monitoring and Damage Assessment, Dynamic Threat Awareness	Detect	PM-16, RA-10
Establish Accounts (T1585)	Enhance User Preparedness (CM1159)	Dynamic Threat Awareness	Detect	AT-2(1), AT-2(5), AT-3(3)
	Monitor External Sources (CM2043)	Monitoring and Damage Assessment, Dynamic Threat Awareness	Detect	AU-13, AU-13(3), RA-5(4), RA-10
Obtain Capabilities (T1588)	Enhance User Preparedness (CM1159)	Dynamic Threat Awareness	Detect	AT-2(1), AT-2(5), AT-3(3)
	Monitor External Sources (CM2043)	Monitoring and Damage Assessment, Dynamic Threat Awareness	Detect	PM-16, RA-10
Stage Capabilities (T1608)	Restrict Supply Chain Exposures (CM1162)	Integrity Checks, Provenance Tracking	Detect	SR-5, SR-11
		Monitoring and Damage Assessment	Detect	SR-6(1), SR-10
		Forensic and Behavioral Analysis	Detect, Scrutinize	SR-10
		Predefined Segmentation	Contain	CM-7(7)
	Monitor External Sources (CM2043)	Monitoring and Damage Assessment, Dynamic Threat Awareness	Detect	PM-16, RA-10
Supply Chain Compromise (T1195)	Restrict Supply Chain Exposures (CM1162)	Integrity Checks, Provenance Tracking	Detect	SR-5, SR-11
		Monitoring and Damage Assessment	Detect	SR-6(1), SR-10
		Forensic and Behavioral Analysis	Detect, Scrutinize	SR-10
		Predefined Segmentation	Contain	CM-7(7)

3095 **TABLE F-5: POTENTIAL EFFECTS OF CYBER RESILIENCY ON INITIAL ACCESS**

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Drive-By Compromise (T1189)	Application Isolation and Sandboxing (M1048)	Predefined Segmentation	Contain, Exert	AC-4(21), AC-6(4), SC-18(5), SC-39, CM-7(6)
	Exploit Protection (M1050)	Integrity Checks	Delay, Exert	AC-4(8)
		Behavior Validation	Detect, Exert	IR-4(13)
	Active Decoys (CM1123)	Misdirection	Deceive, Negate, Contain	SC-26
		Misdirection	Detect, Scrutinize	SC-35
		Dynamic Segmentation and Isolation	Contain	SC-35
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
	Endpoint Behavior Analysis (CM2003)	Monitoring and Damage Assessment	Detect	AC-2(12)
Exploit Public-Facing Application (T1190)	Application Isolation and Sandboxing (M1048)	Predefined Segmentation	Contain, Exert	AC-4(21), AC-6(4), SC-18(5), SC-39, CM-7(6)
	Privileged Account Management (M1026)	Trust-Based Privilege Management	Negate, Exert	AC-6(2)
	Monitor Logs (CM2004)	Behavior Validation	Detect	AU-6
	Present Deceptive Information (CM1101)	Disinformation	Delay, Deter, Deceive, Exert	SC-30(4)
	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
External Remote Services (T1133)	Disable or Remove Feature or Program (M1042)	Restriction	Preempt, Negate	CM-7(2)
	Enhanced Authentication (CM1126)	Calibrated Defense-in-Depth, Path Diversity	Delay, Exert	IA-2(13)
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Connectivity	Preempt, Shorten	SC-10, SI-14(3)
	Minimize Data Retention or (CM1124)	Non-Persistent Information	Degrade, Preempt	SC-23(3)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Analyze Logs (CM2005)	Monitoring and Damage Assessment, Behavior Validation	Detect	SI-4(13)
		Sensor Fusion and Analysis	Detect	SI-4(16)
Hardware Additions (T1200)	Limit Access to Resource over Network (M1035)	Trust-Based Privilege Management	Preempt	AC-6(3), AC-6(10)
	Limit Hardware Installation (M1034)	Restriction	Preempt, Negate	CM-8(3)
	Authenticate Devices (CM1125)	Obfuscation, Integrity Checks	Preempt, Negate	IA-3(1)
	Host Event Detection (CM2007)	Monitoring and Damage Assessment	Detect	CM-8(3)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Preempt	SC-30(4)
Phishing (T1566)	User Training (M1017)	Dynamic Threat Awareness	Negate, Exert	AT-2(1), AT-2(3), AT-2(5)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Preempt	SC-30(4)
	Detonation Chamber (CM1103)	Forensic and Behavioral Analysis	Detect, Scrutinize	SC-44
		Misdirection	Divert, Negate	SC-44
		Predefined Segmentation	Contain, Delay, Exert	SC-44
	Active Decoys (CM1123)	Misdirection	Deceive, Negate, Contain	SC-26
		Misdirection	Detect, Scrutinize	SC-35, SC-44
		Dynamic Segmentation and Isolation	Contain	SC-35, SC-44
Replication Through Removable Media (T1091)	Disable or Remove Feature or Program (M1042)	Restriction	Exert, Preempt	CM-7(2)
	Virtual Sandbox (CM1109)	Non-Persistent Services	Preempt, Shorten	SC-7(20)
		Dynamic Segmentation and Isolation	Delay, Contain	SC-7(20)
	Removable Device Usage Detection (CM2008)	Monitoring and Damage Assessment	Detect	CM-8(3)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Supply Chain Compromise (T1195)	Software Integrity Check (CM2009)	Integrity Checks	Detect	SI-7, SI-7(1)
		Integrity Checks, Provenance Tracking	Detect	CM-14, SR-4(3)
	Software Stress Testing (CM2010)	Self-Challenge	Detect	SR-6(1)
	Physical Inspection (CM2011)	Integrity Checks	Detect	SR-9, SR-10
	Component Provenance Validation (CM1105)	Provenance Tracking	Detect, Delay, Exert	SR-4, SR-4(1), SR-4(2), SR-4(3), SR-4(4)
	Supply Chain Diversity (CM1106)	Supply Chain Diversity	Exert	PL-8(2), SR-3(1), SR-3(2)
Trusted Relationship (T1199)	Network Segmentation (M1030)	Predefined Segmentation	Contain, Exert	SC-7, SC-7(21)
	Monitor Trusted Parties (CM2012)	Dynamic Threat Awareness	Detect	PM-16
		Behavior Validation	Detect	SI-10(3)
		Provenance Tracking	Detect	PM-30(1)
Valid Accounts (T1078)	Privileged Account Management (M1026)	Trust-Based Privilege Management, Consistency Analysis	Preempt	AC-6(7)
	Present Deceptive Information (CM1101)	Disinformation	Exert	SC-30(4)
		Tainting	Detect	SI-20
	Cross-Enterprise Account Usage Analysis (CM2013)	Sensor Fusion and Analysis	Detect	AU-6(3), SI-4(16)

TABLE F-6: POTENTIAL EFFECTS OF CYBER RESILIENCY ON EXECUTION

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Command and Scripting Interpreter (T1059)	Code Signing (M1045)	Provenance Tracking	Preempt	SI-7(15)
	Disable or Remove Feature or Program (M1042)	Restriction	Exert, Preempt	CM-7(2), SC-3(3)
	Execution Prevention (M1038)	Purposing	Negate, Delay, Degrade, Exert	CM-7(4), CM-7(5)
	Monitor Script Execution (CM2029)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(13)
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(13)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Minimize Local Functionality (CM1119)	Restriction	Preempt, Contain	SC-25
	Quarantine or Delete Suspicious Files (CM1132)	Provenance Tracking	Detect	SR-4(3)
		Dynamic Segmentation and Isolation	Contain, Delay, Degrade, Exert	CM-7(6)
		Non-Persistent Information	Expunge	SI-14, SI-14(2)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26, SI-3(10)
Container Administration Command (T1609)	Execution Prevention (M1038)	Non-Persistent Services, Provenance Tracking	Negate, Exert	SI-14(1)
	Execution Prevention (CM1111)	Attribute-Based Usage Restriction	Degrade, Exert	AC-3(13)
	Analyze Logs (CM2005)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12), SI-4(16)
Deploy Container (T1610)	Network Segmentation (M1030)	Predefined Segmentation	Contain, Exert	SC-7
	User Account Management (M1018)	Trust-Based Privilege Management	Degrade, Exert	AC-6(7)
	Calibrate Administrative Access (CM1164)	Attribute-Based Usage Restriction	Degrade, Exert	AC-6
		Trust-Based Privilege Management	Degrade, Exert	AC-6(5)
		Restriction	Degrade, Exert	CM-7(2)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Analyze Logs (CM2005)	Sensor Fusion and Analysis	Detect	SI-4(16)
	Host Event Detection (CM2007)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Exploitation for Client Execution (T1203)	Application Isolation and Sandboxing (M1048)	Predefined Segmentation	Negate, Delay, Degrade, Exert	AC-4(21), AC-6(4), SC-39, CM-7(6)
	Detonation Chamber (CM1103)	Predefined Segmentation	Negate	SC-44
	Endpoint Behavior Analysis (CM2003)	Monitoring and Damage Assessment	Detect	AC-2(12)
	Endpoint Scrutiny (CM2019)	Forensic and Behavioral Analysis	Scrutinize, Detect	IR-4(12)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
Inter-Process Communication (T1559)	Behavior Prevention on Endpoint (M1040)	Restriction	Exert, Preempt	CM-7(2)
	Disable or Remove Feature or Program (M1042)	Restriction	Exert, Preempt	CM-7(2)
	Network Segmentation (M1030)	Predefined Segmentation	Negate	SC-7
	Monitor Use of Libraries and Utilities (CM2040)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4), SI-4(13)
	Monitor Network Usage (CM2047)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Monitoring and Damage Assessment	Detect	SI-4(11), SI-4(13)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
Native API (T1106)	Execution Prevention (M1038)	Purposing	Negate, Delay, Degrade, Exert	CM-7(5)
	Host-Local Event Correlation (CM2022)	Sensor Fusion and Analysis	Detect	IR-4(13), SI-4(16)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
Scheduled Task/Job (T1053)	Passive Decoys (CM1104)	Misdirection	Deceive, Detect, Scrutinize	SC-26
	Monitor Logs (CM2004)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Monitor Specific Files (CM2035)	Monitoring and Damage Assessment	Detect	AU-6
Shared Modules (T1129)	Execution Prevention (M1038)	Purposing	Negate, Delay, Degrade, Exert	CM-7(5)
	Execution Restriction (CM1111)	Attribute-Based Usage Restriction	Negate, Delay, Degrade, Exert	AC-3(13)
	Host-Local Event Correlation (CM2022)	Sensor Fusion and Analysis	Detect	IR-4(13), SI-4(16)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
Software Deployment Tools (T1072)	Privileged Account Management (M1026)	Trust-Based Privilege Management	Exert	AC-6(5)
	Remote Data Storage (M1029)	Predefined Segmentation, Trust-Based Privilege Management	Exert	AC-6(4)
	User Account Management (M1018)	Trust-Based Privilege Management	Degrade, Exert, Shorten, Reduce	AC-6(7)
		Consistency Analysis	Degrade, Exert, Shorten, Reduce	AC-6(7)
	Isolate or Contain Selected Applications or Components (CM1133)	Trust-Based Privilege Management	Degrade, Exert, Shorten, Reduce	CM-7(6)
		Predefined Segmentation	Contain	CM-7(6)
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services	Expunge, Shorten	SI-14(1)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Monitor Trusted Parties (CM2012)	Dynamic Threat Awareness	Detect	PM-16
		Provenance Tracking	Detect	PM-30(1)
		Dynamic Resource Awareness	Detect	SI-4(17)
	Cross-Enterprise Behavior Analysis (CM2018)	Sensor Fusion and Analysis	Detect	AU-6(5), AU-6(3)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
System Services (T1569)	Privileged Account Management (M1026)	Trust-Based Privilege Management	Negate, Exert	AC-6(8)
	User Account Management (M1018)	Attribute-Based Usage Restriction	Negate, Exert	AC-3(13)
	Monitor Logs (CM2004)	Monitoring and Damage Assessment	Detect	AU-6
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Monitor Specific Files (CM2035)	Monitoring and Damage Assessment	Detect	AU-6
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
User Execution (T1204)	Restrict Web-Based Content (M1021)	Integrity Checks	Preempt, Exert	AC-4(8)
	Minimize Local Functionality (CM1119)	Restriction	Contain, Preempt	CM-7(2), SC-25
	Identify External Malware (CM1136)	Monitoring and Damage Assessment	Detect	SC-35
		Forensic and Behavioral Analysis	Scrutinize	SC-35
		Misdirection	Detect, Scrutinize	SC-35
		Dynamic Segmentation and Isolation	Contain	SC-35
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Windows Management Instrumentation (T1047)	Privileged Account Management (M1026)	Trust-Based Privilege Management	Negate, Degrade, Delay, Exert	AC-6(5)
		Trust-Based Privilege Management	Negate, Degrade, Delay, Exert	AC-6(7)
		Consistency Analysis	Degrade, Delay, Exert	AC-6(7)
	Calibrate Administrative Access (CM1164)	Attribute-Based Usage Restriction	Exert	AC-6
		Trust-Based Usage Restriction	Exert	AC-6(5)
		Restriction	Exert	CM-7(2)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26

3099
3100
3101 **TABLE F-7: POTENTIAL EFFECTS OF CYBER RESILIENCY ON PERSISTENCE**

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Account Manipulation (T1098)	Network Segmentation (M1030)	Predefined Segmentation	Contain, Delay, Preempt	AC-4(21), SC-7(20)
	Privileged Account Management (M1026)	Trust-Based Privilege Management	Negate, Delay, Degrade, Exert	AC-6(2)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Detect	SI-20
	Cross-Enterprise Behavior Analysis (CM2018)	Sensor Fusion and Analysis	Detect	AU-6(5)
	Enhanced Authentication (CM1126)	Calibrated Defense-in-Depth, Path Diversity	Degrade, Exert	IA-2(13)
	Account Monitoring (CM2021)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)
BITS Jobs (T1197)	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Disinformation	Deceive	SC-30(4)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Boot or Logon Autostart Execution (T1547)	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Passive Decoys (CM1104)	Misdirection	Deceive, Negate, Contain	SC-26
	Lock Down Thin Nodes (CM1115)	Non-Persistent Services	Preempt	SC-25
		Non-Persistent Information	Preempt	SC-25, SC-34(1)
		Restriction	Preempt	SC-25
		Integrity Checks	Preempt	SC-34
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Information	Expunge, Negate	SI-14(2)
	Monitor Platform Status (CM2044)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Boot or Logon Initialization Scripts (T1037)	Passive Decoys (CM1104)	Misdirection	Deceive, Negate, Contain	SC-26
	Lock Down Thin Nodes (CM1115)	Non-Persistent Services	Preempt	SC-25
		Non-Persistent Information	Preempt	SC-25, SC-34(1)
		Restriction	Preempt	SC-25
		Integrity Checks	Preempt	SC-34
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services	Expunge, Negate	SI-14(1)
	Monitor Script Execution (CM2029)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(13)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Monitor Platform Status (CM2044)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Browser Extensions (T1176)	Audit (M1047)	Provenance Tracking	Detect, Negate	AU-10(2)
	Active Decoys (CM1123)	Misdirection	Deceive, Negate, Contain	SC-26
		Misdirection	Detect, Scrutinize	SC-35
		Dynamic Segmentation and Isolation	Contain	SC-35
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment	Detect	IR-4(13)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Compromise Client Software Binary (T1554)	Code Signing (M1045)	Provenance Tracking	Detect	SI-7(15)
	Lock Down Thin Nodes (CM1115)	Non-Persistent Services	Preempt	SC-25
		Non-Persistent Information	Preempt	SC-25, SC-34(1)
		Restriction	Preempt	SC-25
		Integrity Checks	Preempt	SC-34
	Endpoint Scrutiny (CM2019)	Forensic and Behavioral Analysis	Detect, Scrutinize	IR-4(12)
	Software Integrity Check (CM2009)	Integrity Checks	Detect, Scrutinize	SI-7(1), SI-7(6)
Create Account (T1136)	Check Policy Consistency (CM1129)	Consistency Analysis	Degrade, Exert, Detect	CA-7(5)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Create or Modify System Process (T1543)	Audit (M1047)	Consistency Analysis	Detect	CA-7(5)
	Passive Decoys (CM1104)	Misdirection	Deceive, Negate, Contain	SC-26
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services	Expunge, Shorten	SI-14(1)
	Software Integrity Check (CM2009)	Integrity Checks	Detect	SI-7, SI-7(1)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Event Triggered Execution (T1546)	Monitor Specific Files (CM2035)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Passive Decoys (CM1104)	Misdirection	Deceive, Negate, Contain	SC-26
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services	Expunge, Shorten	SI-14(1)
	Software Integrity Check (CM2009)	Integrity Checks	Detect	SI-7, SI-7(1)
External Remote Services (T1133)	Disable or Remove Feature or Program (M1042)	Restriction	Preempt, Negate	CM-7(2)
	Enhanced Authentication (CM1126)	Calibrated Defense-in-Depth, Path Diversity	Delay, Exert	IA-2(13)
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Connectivity	Expunge, Shorten	SC-10, SI-14(3)
	Minimize Data Retention or Lifespan (CM1124)	Non-Persistent Information	Exert, Preempt	SC-23(3)
	Monitor Logs (CM2004)	Monitoring and Damage Assessment	Detect	AU-6
Hijack Execution Flow (T1574)	Audit (M1047)	Non-Persistent Information	Preempt, Exert	SI-14(2)
	Execution Prevention (M1038)	Purposing	Negate, Delay, Degrade, Exert	CM-7(5)
	Restrict File and Directory Permissions (M1022)	Integrity Checks	Preempt, Exert	SC-34
	Active Decoys (CM1123)	Misdirection	Deceive, Negate, Contain	SC-26
		Misdirection	Detect, Scrutinize	SC-35
		Dynamic Segmentation and Isolation	Contain	SC-35
	Validate Data Properties (CM1137)	Integrity Checks	Detect	SI-7, SI-7(1)
		Calibrated Defense-in-Depth	Delay, Degrade	PL-8(1)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
		Sensor Fusion and Analysis	Detect	SI-4(24)
Implant Container Image (T1525)	Audit (M1047)	Integrity Checks	Detect	SI-7, SI-7(1)
	Code Signing (M1045)	Provenance Tracking	Preempt	SI-7(15)
	Account Monitoring (CM2021)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services	Expunge, Shorten	SI-14(1)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Office Application Startup (T1137)	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services	Expunge, Shorten	SI-14(1)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Pre-OS Boot (T1542)	Boot Integrity (M1046)	Integrity Checks	Detect	SI-6, SI-7, SI-7(1), SI-7(9)
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Information	Expunge, Shorten	SI-14(1)
	Endpoint Scrutiny (CM2019)	Forensic and Behavioral Analysis	Detect	IR-4(12)
	Hardware-Based Protection of Firmware (CM1154)	Integrity Checks	Negate, Preempt	SC-51
	Host-Local Event Correlation (CM2022)	Sensor Fusion and Analysis	Detect	IR-4(13), SI-4(16)
Scheduled Task/Job (T1053)	Passive Decoys (CM1104)	Misdirection	Deceive, Detect, Scrutinize	SC-26
	Monitor Logs (CM2004)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6
	Monitor Specific Files (CM2035)	Monitoring and Damage Assessment	Detect	AU-6

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Server Software Component (T1505)	Audit (M1047)	Integrity Checks	Detect	SI-7, SI-7(1)
	Code Signing (M1045)	Provenance Tracking	Preempt	SI-7(15)
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12)
		Sensor Fusion and Analysis	Detect	SI-4(16)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Traffic Signaling (T1205)	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Connectivity	Preempt, Exert	SC-10, SI-14(3)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Valid Accounts (T1078)	Privileged Account Management (M1026)	Trust-Based Privilege Management, Consistency Analysis	Degrade, Exert, Shorten, Reduce	AC-6(7)
		Consistency Analysis	Degrade, Exert, Shorten, Reduce	AC-6(7)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Detect	SI-20
	Cross-Enterprise Account Usage Analysis (CM2013)	Sensor Fusion and Analysis	Detect	AU-6(3), SI-4(16)

TABLE F-8: POTENTIAL EFFECTS OF CYBER RESILIENCY ON PRIVILEGE ESCALATION

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Abuse Elevation Control Mechanism (T1548)	Execution Prevention (M1038)	Purposing	Negate	CM-7(5)
	Partition Host (CM1118)	Predefined Segmentation	Delay, Negate, Contain	SC-2, SC-2(1), SC-32, SC-32(1)
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Access Token Manipulation (T1134)	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-26, SC-30(4)
		Tainting	Detect, Scrutinize	SI-20
	Partition Host (CM1118)	Predefined Segmentation	Delay, Negate, Contain	SC-2, SC-2(1), SC-32, SC-32(1)
	Enhanced Authentication (CM1126)	Adaptive Management, Calibrated Defense-in-Depth, Dynamic Privileges	Delay, Exert	IA-10
		Architectural Diversity, Design Diversity, Adaptive Management	Delay, Exert	CP-13
		Path Diversity	Delay, Exert	SC-47
	Validate Data Properties (CM1137)	Integrity Checks	Negate, Detect	SC-16(1), SC-16(3)
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Process Analysis (CM2014)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Boot or Logon Autostart Execution (T1547)	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Passive Decoys (CM1104)	Misdirection	Deceive, Negate, Contain	SC-26
	Lock Down Thin Nodes (CM1115)	Non-Persistent Services	Preempt	SC-25
		Non-Persistent Information	Preempt	SC-25, SC-34(1)
		Restriction	Preempt	SC-25
		Integrity Checks	Preempt	SC-34
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Information	Expunge, Negate	SI-14(2)
	Monitor Platform Status (CM2044)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Boot or Logon Initialization Scripts (T1037)	Passive Decoys (CM1104)	Misdirection	Deceive, Negate, Contain	SC-26
	Lock Down Thin Nodes (CM1115)	Non-Persistent Services	Preempt	SC-25
		Non-Persistent Information	Preempt	SC-25, SC-34(1)
		Restriction	Preempt	SC-25
		Integrity Checks	Preempt	SC-34
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services	Expunge, Negate	SI-14(1)
	Monitor Script Execution (CM2029)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(13)
	Monitor Platform Status (CM2044)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Create or Modify System Process (T1543)	Audit (M1047)	Consistency Analysis	Detect	CA-7(5)
	Passive Decoys (CM1104)	Misdirection	Deceive, Negate, Contain	SC-26
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services	Expunge, Shorten	SI-14(1)
	Software Integrity Check (CM2009)	Integrity Checks	Detect	SI-7, SI-7(1)
Escape to Host (T1611)	Application Isolation and Sandboxing (M1048)	Restriction	Contain, Exert	CM-7(2)
	Execution Prevention (M1038)	Non-Persistent Services	Negate, Exert	SC-34, SC-34(1)
	Privileged Account Management (M1026)	Attribute-Based Usage Restriction	Exert	AC-6
	Analyze Logs (CM2005)	Sensor Fusion and Analysis	Detect	SI-4(16)
	Host Event Detection (CM2007)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Event Triggered Execution (T1546)	Monitor Specific Files (CM2035)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Passive Decoys (CM1104)	Misdirection	Deceive, Negate, Contain	SC-26
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services	Expunge, Shorten	SI-14(1)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Software Integrity Check (CM2009)	Integrity Checks	Detect	SI-7, SI-7(1)
Exploitation for Privilege Escalation (T1068)	Application Isolation and Sandboxing (M1048)	Predefined Segmentation	Contain, Exert	AC-4(21), AC-6(4), SC-18(5), SC-39, CM-7(6)
	Exploit Protection (M1050)	Integrity Checks	Delay, Exert	AC-4(8)
		Behavior Validation	Detect, Exert	IR-4(13)
	Threat Intelligence Program (M1019)	Dynamic Threat Awareness	Exert, Preempt	PM-16, RA-3(3)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Exert, Scrutinize, Reveal[134]	SI-20
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Information	Expunge, Shorten	SI-14(1)
	Endpoint Behavior Analysis (CM2003)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)
Group Policy Modification (T1484)	User Account Management (M1018)	Attribute-Based Usage Restriction	Negate, Exert	AC-3(13)
	Passive Decoys (CM1104)	Misdirection	Deceive, Detect	SC-26
	Lock Down Visibility or Access (CM1149)	Attribute-Based Usage Restriction	Negate, Exert	AC-3(11)
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12)
Hijack Execution Flow (T1574)	Audit (M1047)	Non-Persistent Information	Preempt, Exert	SI-14(2)
	Execution Prevention (M1038)	Purposing	Negate, Delay, Degrade, Exert	CM-4(4), CM-7(5)
	Restrict File and Directory Permissions (M1022)	Integrity Checks	Preempt, Exert	SC-34
	Active Decoys (CM1123)	Misdirection	Deceive, Negate, Contain	SC-26
		Misdirection	Detect, Scrutinize	SC-35
		Dynamic Segmentation and Isolation	Contain	SC-35

[134] The Reveal effect is identified only for some uses of CM1101. Reveal can be an effect if the organization uses the PM-16 control—which is cited by M1019, CM2012, and CM1301—to share threat information that it develops with other organizations rather than simply being a consumer of threat information developed by other organizations.

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Validate Data Properties (CM1137)	Integrity Checks	Detect	SI-7, SI-7(1)
		Calibrated Defense-in-Depth	Delay, Degrade	PL-8(1)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
		Sensor Fusion and Analysis	Detect	SI-4(24)
Process Injection (T1055)	Privileged Account Management (M1026)	Trust-Based Privilege Management	Negate, Degrade	AC-6(7)
		Attribute-Based Usage Restriction	Negate, Degrade	AC-6(8)
	Dynamically Relocate and Refresh Processing (CM1150)	Functional Relocation of Cyber Resources	Shorten	SC-30(3)
		Non-Persistent Services	Shorten	SI-14(1)
	Host Event Detection (CM2007)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Process Analysis (CM2014)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Scheduled Task/Job (T1053)	Passive Decoys (CM1104)	Misdirection	Deceive, Detect, Scrutinize	SC-26
	Monitor Logs (CM2004)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6
	Monitor Specific Files (CM2035)	Monitoring and Damage Assessment	Detect	AU-6
Valid Accounts (T1078)	Privileged Account Management (M1026)	Trust-Based Privilege Management	Degrade, Exert, Shorten, Reduce	AC-6(7)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Detect	SI-20
	Cross-Enterprise Account Usage Analysis (CM2013)	Sensor Fusion and Analysis	Detect	AU-6(3) SI-4(16)

3108 **TABLE F-9: POTENTIAL EFFECTS OF CYBER RESILIENCY ON DEFENSE EVASION**

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Abuse Elevation Control Mechanism (T1548)	Execution Prevention (M1038)	Purposing	Negate	CM-7(5)
	Partition Host (CM1118)	Predefined Segmentation	Delay, Negate, Contain	SC-2, SC-2(1), SC-32, SC-32(1)
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Access Token Manipulation (T1134)	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-26, SC-30(4)
		Tainting	Detect, Scrutinize	SI-20
	Partition Host (CM1118)	Predefined Segmentation	Delay, Negate, Contain	SC-2, SC-2(1), SC-32, SC-32(1)
	Validate Data Properties (CM1137)	Integrity Checks	Negate, Detect	SC-16(1), SC-16(3)
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Process Analysis (CM2014)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
BITS Jobs (T1197)	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Build Image on Host (T1612)	Audit (M1047)	Integrity Checks	Detect	SI-7, SI-7(1)
	Network Segmentation (M1030)	Predefined Segmentation	Negate, Degrade, Exert	SC-7
	Execution Prevention (CM1111)	Attribute-Based Usage Restriction	Degrade, Exert	AC-3(12)
	Lock Down Visibility or Access (CM1149)	Attribute-Based Usage Restriction	Negate, Exert	AC-3(11)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Deobfuscate/ Decode Files or Information (T1140)	Application- or Utility-Specific Data Removal (CM1110)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
		Integrity Checks	Detect	SI-7(1), SI-7(7)
		Dynamic Reconfiguration	Expunge	IR-4(2)
	Host-Local Event Correlation (CM2022)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(16)
Deploy Container (T1610)	Network Segmentation (M1030)	Predefined Segmentation	Contain, Exert	SC-7
	User Account Management (M1018)	Trust-Based Privilege Management	Degrade, Exert	AC-6(7)
	Calibrate Administrative Access (CM1164)	Attribute-Based Usage Restriction	Degrade, Exert	AC-6
		Trust-Based Privilege Management	Degrade, Exert	AC-6(5)
		Restriction	Degrade, Exert	CM-7(2)
	Analyze Logs (CM2005)	Sensor Fusion and Analysis	Detect	SI-4(16)
	Host Event Detection (CM2007)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Direct Volume Access (T1006)	Present Decoy Data (CM1113)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect, Scrutinize	SI-20
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Monitor Script Execution (CM2029)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(13)
Execution Guardrails (T1480)	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
Exploitation for Defense Evasion (T1211)	Application Isolation and Sandboxing (M1048)	Predefined Segmentation	Contain, Exert	AC-4(21), AC-6(4), SC-39, CM-7(6)
	Exploit Protection (M1050)	Integrity Checks	Delay, Exert	AC-4(8)
	Threat Intelligence Program (M1019)	Dynamic Threat Awareness	Exert, Preempt	PM-16, RA-3(3)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
File and Directory Permissions Modification (T1222)	Privileged Account Management (M1026)	Trust-Based Privilege Management	Negate, Delay, Degrade, Exert	AC-6(7)
		Attribute-Based Usage Restriction	Negate, Delay, Degrade, Exert	AC-6(8)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Exert, Scrutinize, Reveal	SI-20
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12)
		Sensor Fusion and Analysis	Detect	SI-4(16)
Group Policy Modification (T1484)	User Account Management (M1018)	Attribute-Based Usage Restriction	Negate, Exert	AC-3(13)
	Passive Decoys (CM1104)	Misdirection	Deceive, Detect	SC-26

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Lock Down Visibility or Access (CM1149)	Attribute-Based Usage Restriction	Negate, Exert	AC-3(11)
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12)
Hide Artifacts (T1564)	Lock Down Thin Nodes (CM1115)	Non-Persistent Services	Preempt	SC-25
		Non-Persistent Information	Preempt	SC-25, SC-34(1)
		Restriction	Preempt	SC-25
		Integrity Checks	Preempt	SC-34
	Monitor Logs (CM2004)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
		Sensor Fusion and Analysis	Detect	SI-4(24)
Hijack Execution Flow (T1574)	Audit (M1047)	Non-Persistent Information	Preempt, Exert	SI-14(2)
	Execution Prevention (M1038)	Purposing	Negate, Delay, Degrade, Exert	CM-7(5)
	Restrict File and Directory Permissions (M1022)	Integrity Checks	Preempt, Exert	SC-34
	Active Decoys (CM1123)	Misdirection	Deceive, Negate, Contain	SC-26
		Misdirection	Detect, Scrutinize	SC-35
		Dynamic Segmentation and Isolation	Contain	SC-35
	Validate Data Properties (CM1137)	Integrity Checks	Detect	SI-7, SI-7(1)
		Calibrated Defense-in-Depth	Delay, Degrade	PL-8(1)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
		Sensor Fusion and Analysis	Detect	SI-4(24)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Impair Defenses (T1562)	Restrict File and Directory Permissions (M1022)	Attribute-Based Usage Restriction	Negate, Degrade, Exert	AC-6(1)
	User Account Management (M1018)	Attribute-Based Usage Restriction	Negate, Degrade, Exert	AC-6(1)
	Lock Down Thin Nodes (CM1115)	Non-Persistent Services	Preempt	SC-25
		Non-Persistent Information	Preempt	SC-25, SC-34(1)
		Restriction	Preempt	SC-25
		Integrity Checks	Preempt	SC-34
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Indicator Removal on Host (T1070)	Encrypt Sensitive Information (M1041)	Obfuscation	Degrade, Exert	AU-9(3), SC-8(4), SC-28(1)
	Remote Data Storage (M1029)	Predefined Segmentation	Degrade, Exert	AU-9(2)
		Non-Persistent Information	Degrade, Exert	SI-14(2)
		Integrity Checks	Degrade, Exert	AU-9(6)
	Restrict File and Directory Permissions (M1022)	Trust-Based Privilege Management	Degrade, Exert	AU-9(6)
	Passive Decoys (CM1104)	Misdirection	Deceive, Detect	SC-26
	Defend Audit Data (CM1158)	Integrity Checks	Negate	AU-9(1)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Indirect Command Execution (T1202)	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment	Detect	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12)
		Sensor Fusion and Analysis	Detect	SI-4(16)
Masquerading (T1036)	Code Signing (M1045)	Provenance Tracking	Detect	SI-7(15)
	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive	SC-26

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
		Sensor Fusion and Analysis	Detect	SI-4(24)
Modify Authentication Process (T1556)	Privileged Account Management (M1026)	Consistency Analysis, Trust-Based Privilege Management	Degrade, Exert, Shorten	AC-6(7)
	Enhanced Authentication (CM1126)	Adaptive Management, Calibrated Defense-in-Depth, Dynamic Privileges	Delay, Exert	IA-10
		Architectural Diversity, Design Diversity, Adaptive Management	Delay, Exert	CP-13
		Path Diversity	Delay, Exert	SC-47
	Cross-Enterprise Behavior Analysis (CM2018)	Sensor Fusion and Analysis	Detect	AU-6(5)
	Account Monitoring (CM2021)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)
Modify Cloud Compute Infrastructure (T1578)	Centralize and Analyze Instance Logging (CM2023)	Sensor Fusion and Analysis	Detect	AU-6(5), IR-4(4)
Modify Registry (T1112)	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment	Detect	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Monitor Platform Status (CM2044)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Modify System Image (T1601)	Boot Integrity (M1046)	Integrity Checks	Detect	SI-7, SI-7(1), SI-7(6), SI-7(9)
	Code Signing (M1045)	Provenance Tracking	Preempt	SI-7(15), SR-4(3)
	Credential Access Protection (M1043)	Standard practice	Delay, Exert	IA-5(7), SC-28(1)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Privileged Account Management (M1026)	Consistency Analysis, Trust-Based Privilege Management	Negate, Delay, Degrade, Exert	AC-6(5)
	Validate Data Properties (CM1137)	Integrity Checks	Negate, Detect	SC-16(1), SC-16(3)
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services, Non-Persistent Information, Provenance Tracking	Expunge, Exert, Shorten	SI-14(1)
	Software Integrity Check (CM2009)	Integrity Checks	Detect	SI-7(6)
Network Boundary Bridging (T1599)	Filter Network Traffic (M1037)	Adaptive Management	Degrade, Reduce	AC-4(3)
		Dynamic Reconfiguration	Degrade, Reduce	IR-4(2)
		Monitoring and Damage Assessment	Detect	SI-4(4)
	Privileged Account Management (M1026)	Consistency Analysis, Trust-Based Privilege Management	Negate, Delay, Degrade, Exert	AC-6(5
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services, Non-Persistent Information	Expunge, Exert, Shorten	SI-14(1)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
	Enhance via Heterogeneity (CM1305)	Architectural Diversity	Exert	AU-9(7), SC-29, SC-29(1)
	Monitor Platform Status (CM2044)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Obfuscated Files or Information (T1027)	Detonation Chamber (CM1103)	Forensic and Behavioral Analysis	Detect, Scrutinize	SC-44
	Application- or Utility-Specific Data Removal (CM1110)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
		Integrity Checks	Detect	SI-7(1), SI-7(7)
		Dynamic Reconfiguration	Expunge	IR-4(2)
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Pre-OS Boot (T1542)	Boot Integrity (M1046)	Integrity Checks	Detect	SI-6, SI-7, SI-7(1), SI-7(9)
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Information	Expunge, Shorten	SI-14(1)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Hardware-Based Protection of Firmware (CM1154)	Integrity Checks	Negate, Preempt	SC-51
	Endpoint Scrutiny (CM2019)	Forensic and Behavioral Analysis	Detect	IR-4(12)
Process Injection (T1055)	Privileged Account Management (M1026)	Trust-Based Privilege Management	Negate, Degrade	AC-6(7)
		Attribute-Based Usage Restriction	Negate, Degrade	AC-6(8)
	Dynamically Relocate and Refresh Processing (CM1150)	Functional Relocation of Cyber Resources	Shorten	SC-30(3)
		Non-Persistent Services	Shorten	SI-14(1)
	Defend Against Memory Attacks (CM1152)	Synthetic Diversity, Temporal Unpredictability	Negate, Exert	SI-16
	Host Event Detection (CM2007)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Process Analysis (CM2014)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Rogue Domain Controller (T1207)	Validate Data Quality (CM1130)	Integrity Checks	Detect, Shorten	SI-7(1)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Rootkit (T1014)	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Calibrate Administrative Access (CM1164)	Attribute-Based Usage Restriction	Exert	AC-6
		Trust-Based Usage Restriction	Exert	AC-6(5)
		Restriction	Exert	CM-7(2)
	Monitor Platform Status (CM2044)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Signed Binary Proxy Execution (T1218)	Privileged Account Management (M1026)	Trust-Based Privilege Management	Negate, Delay, Degrade, Exert	AC-6(7)
		Attribute-Based Usage Restriction	Negate, Delay, Degrade, Exert	AC-6(8)
	Disable or Remove Feature or Program (M1042)	Restriction	Exert, Preempt	CM-7(2), SC-3(3)
	Minimize Local Functionality (CM1119)	Restriction	Preempt, Contain	SC-25
	Quarantine or Delete Suspicious Files (CM1132)	Provenance Tracking	Detect	SR-4(3)
		Dynamic Segmentation and Isolation	Contain, Delay, Degrade, Exert	CM-7(6)
		Non-Persistent Information	Expunge	SI-14, SI-14(2)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	SI-4(2)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Signed Script Proxy Execution (T1216)	Minimize Local Functionality (CM1119)	Restriction	Preempt, Contain	SC-25
	Quarantine or Delete Suspicious Files (CM1132)	Provenance Tracking	Detect	SR-4(3)
		Dynamic Segmentation and Isolation	Contain, Delay, Degrade, Exert	CM-7(6)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Non-Persistent Information	Expunge	SI-14, SI-14(2)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	SI-4(2)
	Monitor Script Execution (CM2029)	Monitoring and Damage Assessment	Detect	IR-4(13) , SI-4(2), SI-4(13)
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
Subvert Trust Controls (T1553)	Execution Prevention (M1038)	Purposing	Negate, Exert	CM-7(5)
	Software Configuration (M1054)	Provenance Tracking	Negate, Exert	AC-4(17)
	Minimize Local Functionality (CM1119)	Restriction	Preempt, Contain	SC-25
	Minimize Data Retention or Lifespan (CM1124)	Non-Persistent Information	Expunge, Shorten	SC-23(3), SI-14(2), SI-21
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
	Analyze Logs (CM2005)	Monitoring and Damage Assessment, Behavior Validation	Detect	SI-4(13)
	Software Integrity Check (CM2009)	Integrity Checks	Detect	SI-7(6)
Template Injection (T1221)	Antivirus/Antimalware (M1049)	Predefined Segmentation	Negate, Contain	SC-44
	Disable or Remove Feature or Program (M1042)	Restriction	Negate, Degrade	CM-7(2)
	Network Intrusion Prevention (M1031)	Predefined Segmentation	Negate, Contain	SC-44
	Passive Decoys (CM1104)	Misdirection	Deceive, Detect	SC-26
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Traffic Signaling (T1205)	Passive Decoys (CM1104)	Misdirection	Deceive, Detect	SC-26
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Connectivity	Preempt, Exert	SC-10, SI-14(3)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Trusted Developer Utilities Proxy Execution (T1127)	Disable or Remove Feature or Program (M1042)	Restriction	Exert, Preempt	CM-7(2), SC-3(3)
	Execution Prevention (M1038)	Purposing	Exert, Preempt	CM-7(5)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Unused/ Unsupported Cloud Regions (T1535)	Software Configuration (M1054)	Attribute-Based Usage Restriction	Negate	AC-3(13)
	Monitor Logs (CM2004)	Monitoring and Damage Assessment	Detect	AU-6, SI-4(11)
Use Alternate Authentication	Minimize Data Retention or Lifespan (CM1124)	Non-Persistent Information	Exert	SC-23(3), SI-14(2), SI-21

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Material (T1550)		Temporal Unpredictability	Exert	SC-23(3)
	Enhanced Authentication (CM1126)	Calibrated Defense-in-Depth, Dynamic Privileges	Delay, Exert	IA-10
	Cross-Enterprise Account Usage Analysis (CM2013)	Sensor Fusion and Analysis	Detect	AU-6(3), SI-4(16)
Valid Accounts (T1078)	Privileged Account Management (M1026)	Consistency Analysis, Trust-Based Privilege Management	Preempt	AC-6(7)
	Present Deceptive Information (CM1101)	Disinformation	Exert	SC-30(4)
		Tainting	Detect	SI-20
	Cross-Enterprise Account Usage Analysis (CM2013)	Sensor Fusion and Analysis	Detect	AU-6(3), SI-4(16)
Virtualization/ Sandbox Evasion (T1497)	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Active Decoys (CM1123)	Misdirection	Deceive, Negate, Contain	SC-26
		Misdirection	Detect, Scrutinize	SC-35
		Dynamic Segmentation and Isolation	Contain	SC-35
Weaken Encryption (T1600)	Execution Restriction (CM1111)	Attribute-Based Usage Restriction	Negate, Degrade, Exert	AC-3(13)
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services, Non-Persistent Information, Provenance Tracking	Expunge, Exert, Shorten	SI-14(1)
XSL Script Processing (T1220)	Minimize Local Functionality (CM1119)	Restriction	Preempt, Contain	SC-25
	Quarantine or Delete Suspicious Files (CM1132)	Provenance Tracking	Detect	SR-4(3)
		Dynamic Segmentation and Isolation	Contain, Delay, Degrade, Exert	CM-7(6)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Non-Persistent Information	Expunge	SI-14(2)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)

3109
3110
3111

TABLE F-10: POTENTIAL EFFECTS OF CYBER RESILIENCY ON CREDENTIAL ACCESS

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Brute Force (T1110)	Enhanced Authentication (CM1126)	Calibrated Defense-in-Depth, Path Diversity	Degrade, Exert	IA-2(13)
	Design Diversity (CM1128)	Design Diversity	Delay, Exert	SA-17(9)
	Present Deceptive Information (CM1101)	Disinformation	Delay, Deter, Deceive, Exert	SC-30(4)
		Tainting	Detect, Scrutinize	SI-20
	Monitor Logs (CM2004)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6
	Check Policy Consistency (CM1129)	Consistency Analysis	Degrade, Exert	CA-7(5)
Credentials from Password Stores (T1555)	Present Deceptive Information (CM1101)	Disinformation	Delay, Deter, Deceive, Exert	SC-30(4)
		Tainting	Detect, Scrutinize	SI-20
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Exploitation for Credential Access (T1212)	Application Isolation and Sandboxing (M1048)	Predefined Segmentation	Contain, Delay, Preempt	AC-4(21), AC-6(4), SC-39, CM-7(6)
	Exploit Protection (M1050)	Integrity Checks	Delay, Exert	AC-4(8)
	Threat Intelligence Program (M1019)	Dynamic Threat Awareness	Exert, Preempt	PM-16, RA-3(3)
	Endpoint Behavior Analysis (CM2003)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	AC-2(12)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Forced Authentication (T1187)	Endpoint Behavior Analysis (CM2003)	Monitoring and Damage Assessment	Detect	AC-2(12)
Input Capture (T1056)	Trusted Path (CM1120)	Predefined Segmentation	Negate, Contain	SC-11
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Detect, Scrutinize	SI-20
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12), SI-4(16)
		Dynamic Resource Awareness	Detect	SI-4(16)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Man-in-the-Middle (T1557)	Disable or Remove Feature or Program (M1042)	Restriction	Negate, Exert	CM-7(2), SC-3(3)
	Filter Network Traffic (M1037)	Provenance Tracking	Negate, Exert	SC-7(11), SI-10(5)
	Limit Access to Resource Over Network (M1035)	Trust-Based Privilege Management	Negate, Exert	AC-6(3)
	Network Intrusion Prevention (M1031)	Monitoring and Damage Assessment, Behavior Validation	Detect	SI-4(4)
	Network Segmentation (M1030)	Predefined Segmentation	Contain, Degrade, Exert	SC-7
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Modify Authentication Process (T1556)	Privileged Account Management (M1026)	Consistency Analysis, Trust-Based Privilege Management	Negate, Delay, Degrade, Exert	AC-6(7)
	Enhanced Authentication (CM1126)	Adaptive Management, Calibrated Defense-in-Depth, Dynamic Privileges	Delay, Exert	IA-10
		Architectural Diversity, Design Diversity, Adaptive Management	Delay, Exert	CP-13
		Path Diversity	Delay, Exert	SC-47
	Cross-Enterprise Behavior Analysis (CM2018)	Sensor Fusion and Analysis	Detect	AU-6(5)
	Account Monitoring (CM2021)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)
Network Sniffing (T1040)	Encrypt Sensitive Information (M1041)	Obfuscation	Delay, Exert	SC-8(4)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Detect, Scrutinize	SI-20
	Enhanced Authentication (CM1126)	Calibrated Defense-in-Depth, Path Diversity	Degrade, Exert	IA-2(13)
	Privileged Account Monitoring (CM2017)	Monitoring and Damage Assessment	Detect	AC-6(8)[135]
OS Credential Dumping (T1003)	Credential Access Protection (M1043)	Standard practice	Preempt, Exert	IA-5, SC-29(1)
	Operating System Configuration (M1028)	Restriction	Preempt	CM-7(2)
	Privileged Process Integrity (M1025)	Restriction	Preempt	CM-7(2)
	Hide Sensitive Information (CM1135)	Obfuscation	Delay, Exert	SC-28(1)
	Monitor Logs (CM2004)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6

[135] AC-6(8) also applies Predefined Segmentation. However, that aspect of the control is intended to address Defense Evasion.

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13)
	Adversarial Simulation (CM1107)	Self-Challenge	Preempt	CA-8, CA-8(2)
Steal Application Access Token (T1528)	Audit (M1047)	Standard practice		
	Restrict Web-Based Content (M1021)	Trust-Based Privilege Management	Negate, Exert	AC-6(4)
	Enhance User Preparedness (CM1159)	Dynamic Threat Awareness	Detect	AT-2(1), AT-2(3), AT-2(5), AT-3(3)
	Hunt for Malicious Processes (CM2048)	Forensic and Behavioral Analysis	Detect	IR-5
Steal or Forge Kerberos Tickets (T1558)	Encrypt Sensitive Information (M1041)	Obfuscation	Delay, Exert	SC-30
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Exert	SC-30(4)
Steal Web Session Cookie (T1539)	Software Configuration (M1054)	Non-Persistent Information	Degrade, Exert	SI-14(2), SI-21
	Minimize Data Retention or Lifespan (CM1124)	Non-Persistent Information	Expunge, Shorten	SI-14(2)
Two-Factor Authentication Interception (T1111)	Monitor Logs (CM2004)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6
Unsecured Credentials (T1552)	Encrypt Sensitive Information (M1041)	Calibrated Defense-in-Depth, Obfuscation	Negate, Degrade, Exert	SC-28(1), IA-2(6)
	Filter Network Traffic (M1037)	Restriction	Negate, Degrade, Exert	SC-3(3)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Detect, Scrutinize	SI-20
	Partition Host (CM1118)	Predefined Segmentation	Contain, Delay, Exert	SC-2, SC-2(1), SC-32, SC-32(1)
	Cross-Enterprise Behavior Analysis (CM2018)	Sensor Fusion and Analysis	Detect	AU-6(3), AU-6(5)

3115 **TABLE F-11: POTENTIAL EFFECTS OF CYBER RESILIENCY ON DISCOVERY**

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Account Discovery (T1087)	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Exert, Reveal, Scrutinize	SI-20
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Application Window Discovery (T1010)	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Browser Bookmark Discovery (T1217)	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Cloud Infrastructure Discovery (T1580)	User Account Management (M1018)	Trust-Based Privilege Management	Degrade	AC-6
		Consistency Analysis	Exert	AC-6(7)
	Monitor Logs (CM2004)	Monitoring and Damage Assessment	Detect	AU-6
Cloud Service Dashboard (T1538)	User Account Management (M1018)	Trust-Based Privilege Management	Degrade	AC-6
		Consistency Analysis	Exert	AC-6(7)
	Monitor Logs (CM2004)	Monitoring and Damage Assessment	Detect	AU-6
Cloud Service Discovery (T1526)	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
	Passive Decoys (CM1104)	Misdirection	Divert, Deceive, Degrade, Exert	SC-26
		Architectural Diversity	Divert, Deceive, Degrade, Exert	SC-29
	Application- or Utility-Specific Monitoring (CM2020	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Container and Resource Discovery (T1613)	Network Segmentation (M1030)	Predefined Segmentation	Negate, Degrade, Exert	SC-7, SC-7(21)
	User Account Management (M1018)	Attribute-Based Usage Restriction	Degrade	AC-6
		Consistency Analysis	Exert	AC-6(7)
	Defend Audit Data (CM1158)	Predefined Segmentation	Negate, Exert	AU-9(2)
	Centralize and Analyze Instance Logging (CM2023)	Sensor Fusion and Analysis	Detect	AU-6(5), IR-4(4)
Domain Trust Discovery (T1482)	Audit (M1047)	Consistency Analysis	Exert	CA-7(5)
	Network Segmentation (M1030)	Predefined Segmentation	Contain, Exert	AC-4(2), AC-4(21), SC-7
	Present Deceptive Information (CM1101)	Disinformation	Delay, Deter, Deceive, Exert	SC-30(4)
		Tainting	Detect, Scrutinize	SI-20
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
File and Directory Discovery (T1083)	Passive Decoys (CM1104)	Misdirection	Deceive, Divert, Delay	SC-26
	Lock Down Thin Nodes (CM1115)	Restriction	Preempt	SC-25
	Dynamic Data Location (CM1116)	Functional Relocation of Cyber Resources	Preempt	SC-30(3)
		Temporal Unpredictability	Preempt, Exert	SC-30(3)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Network Service Scanning (T1046)	Network Segmentation (M1030)	Predefined Segmentation	Contain, Exert	AC-4(2), AC-4(21), SC-7
	Passive Decoys (CM1104)	Misdirection	Deceive, Divert, Delay	SC-26

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Network Share Discovery (T1135)	Passive Decoys (CM1104)	Misdirection	Deceive, Divert, Delay	SC-26
	Conceal Resources from Discovery (CM1160)	Obfuscation, Functional Relocation of Cyber Resources	Degrade, Exert, Shorten	SC-7(16), SC-30, SC-30(5)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Network Sniffing (T1040)	Encrypt Sensitive Information (M1041)	Obfuscation	Delay, Degrade, Preempt	SC-8(1), SC-8(4)
	Conceal or Randomize Network Traffic (CM1148)	Obfuscation, Contextual Unpredictability	Delay, Exert	SC-8(5), SC-30
	Enhanced Authentication (CM1126)	Calibrated Defense-in-Depth, Path Diversity	Degrade, Exert	IA-2(13)
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Connectivity	Delay, Preempt	SI-14(3)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Password Policy Discovery (T1201)	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Peripheral Device Discovery (T1120)	Lock Down Thin Nodes (CM1115)	Restriction	Preempt	SC-25
	Conceal Resources from Discovery (CM1160)	Obfuscation, Functional Relocation of Cyber Resources	Degrade, Exert, Shorten	SC-7(16), SC-30, SC-30(5)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Permission Groups Discovery (T1069)	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Scrutinize, Reveal	SI-20

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Process Discovery (T1057)	Lock Down Thin Nodes (CM1115)	Restriction	Preempt	SC-25
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Query Registry (T1012)	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Exert, Scrutinize, Reveal	SI-20
	Lock Down Thin Nodes (CM1115)	Restriction	Preempt	SC-25
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Remote System Discovery (T1018)	Passive Decoys (CM1104)	Misdirection	Deceive, Divert, Delay	SC-26
	Conceal Resources from Discovery (CM1160)	Obfuscation, Functional Relocation of Cyber Resources	Degrade, Exert, Shorten	SC-7(16), SC-30, SC-30(5)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Software Discovery (T1518)	Lock Down Thin Nodes (CM1115)	Restriction	Preempt	SC-25
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
System Information Discovery (T1082)	Present Deceptive Information (CM1101)	Disinformation	Deceive, Degrade, Exert	SC-30(4)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
System Location Discovery (T1614)	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Physically Relocate Resources (CM1165)	Asset Mobility	Expunge, Exert	SC-30(3)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13)
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
System Network Configuration Discovery (T1016)	Present Deceptive Information (CM1101)	Disinformation	Deceive, Degrade, Exert	SC-30(4)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
System Network Connections Discovery (T1049)	Conceal Resources from Discovery (CM1160)	Obfuscation, Functional Relocation of Cyber Resources	Degrade, Exert, Shorten	SC-7(16), SC-30, SC-30(5)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
System Owner/User Discovery (T1033)	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Exert, Scrutinize, Reveal	SI-20
	Lock Down Thin Nodes (CM1115)	Restriction	Preempt	SC-25
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Services	Shorten	AC-12
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
System Service Discovery (T1007)	Lock Down Thin Nodes (CM1115)	Restriction	Preempt	SC-25
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
System Time Discovery (T1124)	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2), SI-4(4)

TABLE F-12: POTENTIAL EFFECTS OF CYBER RESILIENCY ON LATERAL MOVEMENT

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Exploitation of Remote Services (T1210)	Application Isolation and Sandboxing (M1048)	Predefined Segmentation	Contain, Delay, Preempt	AC-4(21), AC-6(4), CM-7(6), SC-39,
	Disable or Remove Feature or Program (M1042)	Restriction	Exert, Preempt	CM-7(2)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Exploit Protection (M1050)	Integrity Checks	Delay, Exert, Detect	AC-4(8)
		Behavior Validation	Detect	IR-4(13)
	Network Segmentation (M1030)	Predefined Segmentation	Contain, Exert	AC-4(2), SC-3, SC-7, SC-7(29)
	Threat Intelligence Program (M1019)	Dynamic Threat Awareness	Exert, Preempt	PM-16, RA-3(3)
	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Endpoint Behavior Analysis (CM2003)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)
	Monitor Network Usage (CM2047)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(11), SI-4(13)
Internal Spear-Phishing (T1534)	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Enhance User Preparedness (CM1159)	Dynamic Threat Awareness	Detect	AT-2(1), AT-2(3), AT-2(5), AT-3(3)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Lateral Tool Transfer (T1570)	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Dynamically Restrict Traffic or Isolate Resources (CM1108)	Dynamic Reconfiguration	Contain, Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Dynamic Segmentation and Isolation	Contain, Shorten, Reduce	SC-7(20)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Modulate Information Flows (CM1153)	Design Diversity, Replication	Negate, Exert	AC-4(27), AC-4(30)
		Orchestration	Exert	AC-4(29)
	Lock Down Thin Nodes (CM1115)	Non-Persistent Services	Preempt	SC-25
		Non-Persistent Information	Preempt	SC-25
		Restriction	Preempt	SC-25
		Integrity Checks	Preempt	SC-34
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(24)
Remote Service Session Hijacking (T1563)	Network Segmentation (M1030)	Predefined Segmentation	Contain, Exert	AC-4(2), AC-4(21), SC-7
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Services	Expunge, Shorten	AC-12
	Refresh Sessions or Connections (CM1146)	Non-Persistent Connectivity	Preempt, Shorten	SI-14(3)
		Temporal Unpredictability	Preempt, Shorten	SC-23(3), SC-30(2)
	Account Monitoring (CM2021)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)
Remote Services (T1021)	User Account Management (M1018)	Consistency Analysis, Trust-Based Privilege Management	Delay, Exert	AC-6(7)
	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Dynamically Restrict Traffic or Isolate Resources (CM1108)	Dynamic Reconfiguration	Contain, Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Dynamic Segmentation and Isolation	Contain, Shorten, Reduce	SC-7(20)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Controlled Interfaces (CM1153)	Predefined Segmentation, Trust-Based Privilege Management	Negate, Exert	SC-7(15)
	Cross-Enterprise Behavior Analysis (CM2018)	Sensor Fusion and Analysis	Detect	AU-6(3), AU-6(5)
Replication Through Removable Media (T1091)	Disable or Remove Feature or Program (M1042)	Restriction	Exert, Preempt	CM-7(2)
	Virtual Sandbox (CM1109)	Non-Persistent Services	Preempt Shorten	SI-14
		Dynamic Segmentation and Isolation	Delay, Contain	SC-7(20)
	Removable Device Usage Detection (CM2008)	Monitoring and Damage Assessment	Detect	CM-8(3)
Software Deployment Tools (T1072)	Remote Data Storage (M1029)	Predefined Segmentation, Trust-Based Privilege Management	Exert	AC-6(4)
	User Account Management (M1018)	Trust-Based Privilege Management	Degrade, Exert, Shorten, Reduce	AC-6(7)
		Consistency Analysis	Degrade, Exert, Shorten, Reduce	AC-6(7)
	Isolate or Contain Selected Applications or Components (CM1133)	Trust-Based Privilege Management	Degrade, Exert, Shorten, Reduce	CM-7(6)
		Predefined Segmentation	Contain	CM-7(6)
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services	Expunge, Shorten	SI-14(1)
	Monitor Trusted Parties (CM2012)	Dynamic Threat Awareness	Detect	PM-16
		Dynamic Resource Awareness	Detect	SI-4(17)
	Cross-Enterprise Behavior Analysis (CM2018)	Sensor Fusion and Analysis	Detect	AU-6(5), AU-6(3)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
Taint Shared Content (T1080)	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26, SI-3(10)
	Validate Data Properties (CM1137)	Integrity Checks	Negate, Detect	SI-7
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
		Behavior Validation	Detect	IR-4(13), SI-4(2)
	Monitor Specific Files (CM2035)	Monitoring and Damage Assessment	Detect	AU-6
Use Alternate Authentication Material (T1550)	Minimize Data Retention or Lifespan (CM1124)	Non-Persistent Information	Exert	SC-23(3), SI-14(2), SI-21
		Temporal Unpredictability	Exert	SC-23(3)
	Enhanced Authentication (CM1126)	Calibrated Defense-in-Depth, Dynamic Privileges	Delay, Exert	IA-10

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Cross-Enterprise Account Usage Analysis (CM2013)	Sensor Fusion and Analysis	Detect	AU-6(3), SI-4(16)

3119
3120
3121

TABLE F-13: POTENTIAL EFFECTS OF CYBER RESILIENCY ON COLLECTION

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Archive Collected Data (T1560)	Audit (M1047)	Sensor Fusion and Analysis	Detect	AU-6(5)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Audio Capture (T1123)	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Dynamically Disable or Suspend (CM1121)	Non-Persistent Connectivity	Preempt, Delay	SC-15(1)
		Dynamic Reconfiguration	Preempt, Delay	AC-2(8)
Automated Collection (T1119)	Encrypt Sensitive Information (M1041)	Obfuscation	Delay, Degrade, Preempt	SC-28(1)
	Remote Data Storage (M1029)	Predefined Segmentation	Delay	AU-9(2),[136] SC-7(21)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Scrutinize, Reveal	SI-20
	Dynamic Data Location (CM1116)	Functional Relocation of Cyber Resources, Temporal Unpredictability	Negate, Delay, Degrade, Exert	SC-30(3)
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Defend Against Data Mining (CM1157)	Monitoring and Damage Assessment, Trust-Based Privilege Management, Attribute-Based Usage	Delay, Degrade, Exert, Detect	AC-23

[136] AU-9(2) applies only to audit information.

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Restriction, Dynamic Privileges		
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Clipboard Data (T1115)	Cross-Enterprise Behavior Analysis (CM2018)	Sensor Fusion and Analysis	Detect	AU-6(5)
Data from Cloud Storage Object (T1530)	Encrypt Sensitive Information (M1041)	Obfuscation	Delay, Degrade, Preempt	SC-28(1)
	Enhanced Authentication (CM1126)	Calibrated Defense-in-Depth, Dynamic Privileges	Delay, Exert	IA-2(13), IA-10
	Cloud Account Monitoring (CM2016)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)
Data from Configuration Repository (T1602)	Encrypt Sensitive Information (M1041)	Obfuscation	Delay, Degrade, Preempt	SC-28(1)
	Network Segmentation (M1030)	Predefined Segmentation	Contain, Exert	SC-7, SC-7(21)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Detect	SC-30(4)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Data from Information Repositories (T1213)	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Scrutinize, Reveal	SI-20
	Adversarial Simulation (CM1107)	Self-Challenge	Negate	SI-19(8)
	Minimize Data Retention or Lifespan (CM1124)	Non-Persistent Information	Delay, Exert, Preempt	SI-14(2), SI-21
	Hide Sensitive Information (CM1135)	Obfuscation	Preempt, Negate, Exert	SI-19(4)
	Privileged Account Monitoring (CM2017)	Monitoring and Damage Assessment	Detect	AC-6(8)
	Account Monitoring (CM2021)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Dynamic Account Management (CM1117)	Dynamic Reconfiguration	Contain, Shorten, Reduce	AC-2(6)
		Dynamic Privileges	Exert, Delay	AC-2(6), AC-2(8)
Data from Local System (T1005)	Partition Host (CM1118)	Predefined Segmentation	Contain, Degrade, Exert	SC-2, SC-2(1), SC-32, SC-32(1)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Hide Sensitive Information (CM1135)	Obfuscation	Delay, Degrade, Preempt	SC-28(1)
Data from Network Shared Drive (T1039)	Partition Host (CM1118)	Predefined Segmentation	Contain, Degrade, Exert	SC-32
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Scrutinize, Reveal	SI-20
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Connectivity	Delay, Preempt	SI-14(3)
	Hide Sensitive Information (CM1135)	Obfuscation	Delay, Degrade, Preempt	SC-28(1)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Data from Removable Media (T1025)	Minimize Local Functionality (CM1119)	Restriction	Preempt, Contain	SC-25
	Dynamically Disable or Suspend (CM1121)	Adaptive Management, Dynamic Reconfiguration	Preempt, Delay	AC-2(8)
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Data Staged (T1074)	Dynamic Data Location (CM1116)	Functional Relocation of Cyber Resources, Temporal Unpredictability	Preempt, Delay, Degrade, Exert	SC-30(3)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Covert Signaling (CM1112)	Tainting	Detect, Reveal	SI-20
Email Collection (T1114)	Encrypt Sensitive Information (M1041)	Obfuscation	Degrade, Exert	SC-8(4)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Scrutinize, Reveal	SI-20
	Enhanced Authentication (CM1126)	Calibrated Defense-in-Depth, Path Diversity	Delay, Exert	IA-2(13)
	Monitor Specific Servers (CM2034)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Input Capture (T1056)	Trusted Path (CM1120)[137]	Predefined Segmentation	Contain	SC-11
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12)
		Dynamic Resource Awareness	Detect	SI-4(16)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)

[137] Note that this mitigation applies to the capture of credentials and not to keylogging or other input capture of more general data types. Thus, it mitigates only part of the Input Capture technique.

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Monitor the File System (CM2033)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Man-in-the-Browser (T1185)	User Account Management (M1018)	Attribute-Based Usage Restriction	Negate, Exert	AC-3(13)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Dynamically Disable or Suspend (CM1121)	Non-Persistent Connectivity	Preempt, Delay	SC-15(1)
		Dynamic Reconfiguration	Preempt, Delay	AC-2(8)
Man-in-the-Middle (T1557)	Disable or Remove Feature or Program (M1042)	Restriction	Negate, Exert	CM-7(2), SC-3(3)
	Filter Network Traffic (M1037)	Restriction	Negate, Exert	SC-3(3)
	Limit Access to Resource Over Network (M1035)	Trust-Based Privilege Management	Negate, Exert	AC-6(3)
	Network Intrusion Prevention (M1031)	Monitoring and Damage Assessment, Behavior Validation	Detect	SI-4(4)
	Network Segmentation (M1030)	Predefined Segmentation	Contain, Degrade, Exert	SC-7
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
Screen Capture (T1113)	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Dynamic Resource Awareness	Detect	SI-4(16)
Video Capture (T1125)	Dynamically Disable or Suspend (CM1121)	Adaptive Management, Dynamic Reconfiguration	Preempt, Delay	AC-2(8)
	Trusted Path (CM1120)	Predefined Segmentation	Contain, Delay, Exert	SC-11
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12)
		Dynamic Resource Awareness	Detect	SI-4(16)

TABLE F-14: POTENTIAL EFFECTS OF CYBER RESILIENCY ON COMMAND AND CONTROL

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Application Layer Protocol (T1071)	Isolate or Contain Selected Applications or Components (CM1133)	Predefined Segmentation, Dynamic Segmentation and Isolation	Preempt, Negate, Contain, Exert	CM-7(6)
		Predefined Segmentation	Preempt, Negate, Contain, Exert	SC-7(21)
	Defend Enclave Boundaries (CM1151)	Predefined Segmentation	Negate, Exert	AC-4(21), SC-7(21), SC-7(22)
		Integrity Checks	Negate, Exert	AC-4(8), AC-4(12)
		Provenance Tracking	Negate, Exert	AC-4(17)
	Modulate Information Flows (CM1153)	Design Diversity, Replication	Negate, Exert	AC-4(27), AC-4(30)
		Orchestration	Exert	AC-4(29)
		Predefined Segmentation	Negate, Exert	SC-46
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Communication Through Removable Media (T1092)	Operating System Configuration (M1028)	Restriction	Preempt	CM-7(2)
	Virtual Sandbox (CM1109)	Non-Persistent Services	Preempt Shorten	SI-14
		Dynamic Segmentation and Isolation	Delay, Contain	SC-7(20)
	Removable Device Usage Detection (CM2008)	Monitoring and Damage Assessment	Detect	CM-8(3)
Data Encoding (T1132)	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Data Obfuscation (T1001)	Modulate Information Flows (CM1153)	Design Diversity, Replication	Negate, Exert	AC-4(27), AC-4(30)
		Orchestration	Exert	AC-4(29)
		Predefined Segmentation	Negate, Exert	SC-46
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Dynamic Resolution (T1568)	Restrict Web-Based Content (M1021)	Disinformation	Negate	SC-30(4)
	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Encrypted Channel (T1573)	SSL/TLS Inspection (M1020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
	Defend Enclave Boundaries (CM1151)	Predefined Segmentation	Negate, Exert	AC-4(21), SC-7(21), SC-7(22)
		Integrity Checks	Negate, Exert	AC-4(8)
		Provenance Tracking	Negate, Exert	AC-4(17)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(25)
Fallback Channels (T1008)	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Refresh Sessions or Connections (CM1146)	Non-Persistent Connectivity	Degrade, Exert	SI-14(3)
		Temporal Unpredictability	Degrade, Exert	SC-30(2)
	Defend Enclave Boundaries (CM1151)	Predefined Segmentation	Negate, Exert	AC-4(21), SC-7(21), SC-7(22)
		Integrity Checks	Negate, Exert	AC-4(8)
		Provenance Tracking	Negate, Exert	AC-4(17)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Ingress Tool Transfer (T1105)	Defend Enclave Boundaries (CM1151)	Predefined Segmentation	Negate, Exert	AC-4(21), SC-7(21), SC-7(22)
		Integrity Checks	Negate, Exert	AC-4(8), AC-4(12)
		Provenance Tracking	Negate, Exert	AC-4(17)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Multi-Stage Channels (T1104)	Refresh Sessions or Connections (CM1146)	Non-Persistent Connectivity	Degrade, Exert	SI-14(3)
		Temporal Unpredictability	Degrade, Exert	SC-30(2)
	Defend Enclave Boundaries (CM1151)	Predefined Segmentation	Negate, Exert	AC-4(21), SC-7(21), SC-7(22)
		Integrity Checks	Negate, Exert	AC-4(8), AC-4(12)
		Provenance Tracking	Negate, Exert	AC-4(17)
	Modulate Information Flows (CM1153)	Design Diversity, Replication	Negate, Exert	AC-4(27), AC-4(30)
		Orchestration	Exert	AC-4(29)
		Predefined Segmentation	Negate, Exert	SC-46
	Cross-Enterprise Behavior Analysis (CM2018)	Sensor Fusion and Analysis	Detect	AU-6(3), AU-6(5)
Non-Application Layer Protocol (T1095)	Defend Enclave Boundaries (CM1151)	Predefined Segmentation	Negate, Exert	AC-4(21), SC-7(21), SC-7(22)
		Integrity Checks	Negate, Exert	AC-4(8)
		Provenance Tracking	Negate, Exert	AC-4(17)
	Modulate Information Flows (CM1153)	Design Diversity, Replication	Negate, Exert	AC-4(27), AC-4(30)
		Orchestration	Exert	AC-4(29)
		Predefined Segmentation	Negate, Exert	SC-46
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Non-Standard Port (T1571)	Network Segmentation (M1030)	Predefined Segmentation	Negate, Contain	AC-4(21), SC-7
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Protocol Tunneling (T1572)	Defend Enclave Boundaries (CM1151)	Predefined Segmentation	Negate, Exert	AC-4(21), SC-7(21), SC-7(22)
		Integrity Checks	Negate, Exert	AC-4(8)
		Provenance Tracking	Negate, Exert	AC-4(17)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
	Monitor Network Usage (CM2047)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(11)
		Behavior Validation	Detect	IR-4(13)
		Monitoring and Damage Assessment, Behavior Validation	Detect	SI-4(13)
Proxy (T1090)	SSL/TLS Inspection (M1020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
	Defend Enclave Boundaries (CM1151)	Predefined Segmentation	Negate, Exert	AC-4(21), SC-7(21), SC-7(22)
		Integrity Checks	Negate, Exert	AC-4(8)
		Provenance Tracking	Negate, Exert	AC-4(17)
	Modulate Information Flows (CM1153)	Design Diversity, Replication	Negate, Exert	AC-4(27), AC-4(30)
		Orchestration	Exert	AC-4(29)
		Predefined Segmentation	Negate, Exert	SC-46
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Remote Access Software (T1219)	Passive Decoys (CM1104)	Misdirection	Deceive, Detect	SC-26
	Lock Down Thin Nodes (CM1115)	Non-Persistent Services	Preempt	SC-25

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Non-Persistent Information	Preempt	SC-25, SC-34(1)
		Restriction	Preempt	SC-25
		Integrity Checks	Preempt	SC-34
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Traffic Signaling (T1205)	Passive Decoys (CM1104)	Misdirection	Deceive, Detect	SC-26
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Connectivity	Preempt, Exert	SC-10, SI-14(3)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)
Web Service (T1102)	Passive Decoys (CM1104)	Misdirection	Deceive, Detect	SC-26
	Cross-Enterprise Behavior Analysis (CM2018)	Sensor Fusion and Analysis	Detect	AU-6(3), AU-6(5)
	Analyze Outgoing Traffic Patterns (CM2042)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)

TABLE F-15: POTENTIAL EFFECTS OF CYBER RESILIENCY ON EXFILTRATION

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Automated Exfiltration (T1020)	Adversarial Simulation (CM1107)	Self-Challenge	Detect	CA-8, SC-7(10)
	Covert Signaling (CM1112)	Tainting	Detect, Scrutinize	SI-20
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-30(4), SC-26
		Tainting	Detect, Scrutinize	SI-20
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Modulate Information Flows (CM1153)	Design Diversity, Replication	Negate, Exert	AC-4(27), AC-4(30)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Orchestration	Exert	AC-4(29)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	AU-6, SI-4(4), SI-4(18)
Data Transfer Size Limits (T1030)	Covert Signaling (CM1112)	Tainting	Detect, Reveal	SI-20
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-30(4), SC-26
		Tainting	Detect, Scrutinize	SI-20
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Analyze Outgoing Traffic Patterns (CM2042)	Monitoring and Damage Assessment, Behavior Validation	Detect	SI-4(18), IR-4(13)
	Monitor Network Usage (CM2047)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Exfiltration Over Alternative Protocol (T1048)	Network Intrusion Prevention (M1031)	Monitoring and Damage Assessment, Behavior Validation	Detect, Negate	SI-4(4)
	Network Segmentation (M1030)	Predefined Segmentation	Degrade, Delay, Exert	SC-7
	Covert Signaling (CM1112)	Tainting	Detect, Reveal	SI-20
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-30(4), SC-26
		Tainting	Detect, Scrutinize	SI-20
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
	Analyze Outgoing Traffic Patterns (CM2042)	Monitoring and Damage Assessment, Behavior Validation	Detect	SI-4(18), IR-4(13)
Exfiltration Over C2 Channel (T1041)	Network Intrusion Prevention (M1031)	Monitoring and Damage Assessment, Behavior Validation	Detect, Negate	SI-4(4)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Covert Signaling (CM1112)	Tainting	Detect, Reveal	SI-20
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-30(4), SC-26
		Tainting	Detect, Scrutinize	SI-20
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Connectivity	Delay, Preempt, Shorten, Reduce	SC-7(10), SC-10, SI-14(3)
	Analyze Outgoing Traffic Patterns (CM2042)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
	Monitor Network Usage (CM2047)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Exfiltration Over Other Network Medium (T1011)	Covert Signaling (CM1112)	Tainting	Detect, Reveal	SI-20
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-30(4), SC-26
		Tainting	Detect, Scrutinize	SI-20
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Connectivity	Delay, Preempt, Shorten, Reduce	SC-7(10), SC-10, SI-14(3)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Monitor Specific Files (CM2035)	Monitoring and Damage Assessment	Detect	AU-6
Exfiltration Over Physical Medium (T1052)	Disable or Remove Feature or Program (M1042)	Restriction	Exert, Preempt	CM-7(2)
	Covert Signaling (CM1112)	Tainting	Detect, Reveal	SI-20
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-30(4), SC-26
		Tainting	Detect, Scrutinize	SI-20

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Host Event Detection (CM2007)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Removable Device Usage Detection (CM2008)	Monitoring and Damage Assessment	Detect	CM-8(3)
Exfiltration Over Web Service (T1567)	Covert Signaling (CM1112)	Tainting	Detect, Reveal	SI-20
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-30(4), SC-26
		Tainting	Detect, Scrutinize	SI-20
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Modulate Information Flows (CM1153)	Design Diversity, Replication	Negate, Exert	AC-4(27), AC-4(30)
		Orchestration	Exert	AC-4(29)
	Analyze Outgoing Traffic Patterns (CM2042)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(18)
Scheduled Transfer (T1029)	Network Intrusion Prevention (M1031)	Monitoring and Damage Assessment	Detect	SI-4(4)
	Covert Signaling (CM1112)	Tainting	Detect, Reveal	SI-20
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-30(4), SC-26
		Tainting	Detect, Scrutinize	SI-20
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Modulate Information Flows (CM1153)	Design Diversity, Replication	Negate, Exert	AC-4(27), AC-4(30)
		Orchestration	Exert	AC-4(29)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6, IR-4(13)
	Analyze Outgoing Traffic Patterns (CM2042)	Monitoring and Damage Assessment, Behavior Validation	Detect	SI-4(18), IR-4(13)
Transfer Data to Cloud Account (T1537)	Covert Signaling (CM1112)	Tainting	Detect, Reveal	SI-20
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-30(4), SC-26

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Tainting	Detect, Scrutinize	SI-20
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Cloud Account Monitoring (CM2016)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)

3128
3129
3130

TABLE F-16: POTENTIAL EFFECTS OF CYBER RESILIENCY ON IMPACT

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Account Access Removal (T1531)	Use Alternate Communications (CM1140)	Path Diversity	Shorten, Reduce	AC-7(4), SC-47
	Dynamic Account Management (CM1117)	Dynamic Privilege, Dynamic Reconfiguration	Shorten, Reduce	AC-2(6)
		Dynamic Reconfiguration	Shorten, Reduce	AC-2(8)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Data Destruction (T1485)	Data Backup (M1053)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Replication	Shorten, Reduce	CP-9(6)
	Dynamic Data Location (CM1116)	Functional Relocation of Cyber Resources	Preempt	SC-30(3)
		Temporal Unpredictability	Preempt, Exert	SC-30(3)
	Validate Data Quality (CM1130)	Integrity Checks	Detect	SA-9(7), SI-7(1)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Perform Mission Damage Assessment (CM1122)	Mission Dependency and Status Visualization	Detect, Scrutinize	CP-2(8), RA-9
		Sensor Fusion and Analysis, Mission Dependency and Status Visualization	Detect, Scrutinize	SI-4(1)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Integrity Checks	Detect, Scrutinize	SI-7, SI-7(1)
	Switch to Alternative Data Sources (CM1138)	Information Diversity	Reduce, Shorten	SI-22
		Dynamic Reconfiguration	Contain, Reduce, Shorten	IR-4(2)
	Dynamically Reprovision (CM1139)	Adaptive Management	Shorten, Reduce	AC-4(3)
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
	Reconstruct Compromised Assets (CM1141)	Information Diversity	Exert, Reduce	SI-22
		Fragmentation	Exert, Reduce	SI-23
		Replication	Exert, Reduce	SC-36
		Dynamic Reconfiguration	Reduce, Shorten	IR-4(9)
	Switch to Protected Hot Shadow (CM1142)	Replication	Shorten, Reduce	CP-9(6)
		Predefined Segmentation	Shorten, Reduce	AC-4(2)
		Integrity Checks	Shorten, Reduce	AC-4(8)
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	CP-2(5)
Data Encrypted for Impact (T1486)	Data Backup (M1053)	Protected Backup and Restore	Shorten, Reduce	CP-9, CP-9(8)
		Replication	Shorten, Reduce	CP-9(6)
	Passive Decoys (CM1104)	Misdirection	Deceive, Negate, Contain	SC-26
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Dynamic Data Location (CM1116)	Functional Relocation of Cyber Resources	Preempt	SC-30(3)
		Temporal Unpredictability	Preempt, Exert	SC-30(3)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Perform Mission Damage Assessment (CM1122)	Mission Dependency and Status Visualization	Detect, Scrutinize	CP-2(8), RA-9
		Sensor Fusion and Analysis, Mission Dependency and Status Visualization	Detect, Scrutinize	SI-4(1)
		Integrity Checks	Detect, Scrutinize	SI-7, SI-7(1)
	Switch to Alternative Data Sources (CM1138)	Information Diversity	Reduce, Shorten	SI-22
		Dynamic Reconfiguration	Contain, Reduce, Shorten	IR-4(2)
	Dynamically Reprovision (CM1139)	Adaptive Management	Shorten, Reduce	AC-4(3)
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
	Reconstruct Compromised Assets (CM1141)	Information Diversity	Exert, Reduce	SI-22
		Fragmentation	Exert, Reduce	SI-23
		Replication	Exert, Reduce	SC-36
		Dynamic Reconfiguration	Reduce, Shorten	IR-4(9)
	Switch to Protected Hot Shadow (CM1142)	Replication	Shorten, Reduce	CP-9(6)
		Predefined Segmentation	Shorten, Reduce	AC-4(2)
		Integrity Checks	Shorten, Reduce	AC-4(8)
		Dynamic Reconfiguration,	Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	CP-2(5)
Data Manipulation (T1565)	Network Segmentation (M1030)	Predefined Segmentation	Contain, Exert	AC-4(2), AC-4(21), SC-7(29)
	Encrypt Sensitive Information (M1041)	Obfuscation	Degrade, Exert	SC-28(1)
	Passive Decoys (CM1104)	Misdirection	Deceive, Negate, Contain	SC-26
	Trusted Path (CM1120)	Predefined Segmentation	Negate, Contain	SC-11

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Validate Data Properties (CM1137)	Integrity Checks	Delay, Degrade, Exert	SI-7, SI-7(1)
		Calibrated Defense-in-Depth	Delay, Degrade	PL-8(1)
	Switch to Alternative Data Sources (CM1138)	Information Diversity	Reduce, Shorten	SI-22
		Dynamic Reconfiguration	Contain, Reduce, Shorten	IR-4(2)
	Validate Output Data (CM1155)	Integrity Checks	Detect, Reduce	SI-15
	Analyze File Contents (CM2006)	Forensic and Behavioral Analysis	Detect	SR-10
Defacement (T1491)	Data Backup (M1053)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Replication	Shorten, Reduce	CP-9(6)
		Protected Backup and Restore, Obfuscation, Integrity Checks	Exert	CP-9(8)
	Passive Decoys (CM1104)	Misdirection	Deceive, Negate, Contain	SC-26
	Dynamic Data Location (CM1116)	Functional Relocation of Cyber Resources	Preempt	SC-30(3)
		Temporal Unpredictability	Preempt, Exert	SC-30(3)
	Validate Data Quality (CM1130)	Integrity Checks	Detect	SA-9(7), SI-7(1)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Disk Wipe (T1561)	Data Backup (M1053)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Replication	Shorten, Reduce	CP-9(6)
	Passive Decoys (CM1104)	Misdirection	Deceive, Negate, Contain	SC-26
	Dynamic Data Location (CM1116)	Functional Relocation of Cyber Resources	Preempt	SC-30(3)
		Temporal Unpredictability	Preempt, Exert	SC-30(3)
	Host Event Detection (CM2007)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Perform Mission Damage Assessment (CM1122)	Mission Dependency and Status Visualization	Detect, Scrutinize	CP-2(8), RA-9
		Sensor Fusion and Analysis, Mission Dependency and Status Visualization	Detect, Scrutinize	SI-4(1)
		Integrity Checks	Detect, Scrutinize	SI-7, SI-7(1)
	Switch to Alternative Data Sources (CM1138)	Information Diversity	Reduce, Shorten	SI-22
		Dynamic Reconfiguration	Contain, Reduce, Shorten	IR-4(2)
	Dynamically Reprovision (CM1139)	Adaptive Management	Shorten, Reduce	AC-4(3)
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
	Reconstruct Compromised Assets (CM1141)	Protected Backup and Restore	Exert, Reduce	CP-9
		Information Diversity	Exert, Reduce	SI-22
		Fragmentation	Exert, Reduce	SI-23
		Replication, Distributed Functionality	Exert, Reduce	SC-36
		Dynamic Reconfiguration	Reduce, Shorten	IR-4(9)
	Switch to Protected Hot Shadow (CM1142)	Replication	Shorten, Reduce	CP-9(6)
		Predefined Segmentation	Shorten, Reduce	AC-4(2)
		Integrity Checks	Shorten, Reduce	AC-4(8)
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	CP-2(5)
	Switch to Alternate System or Component (CM1143)	Architectural Diversity	Shorten, Reduce	SC-29
		Design Diversity	Shorten, Reduce	SA-17(9)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	CP-2(5)
	Defend Failover and Recovery (CM1145)	Adaptive Management, Dynamic Reconfiguration, Orchestration	Shorten, Reduce, Exert	IR-4(3)
		Functional Relocation of Sensors	Detect	SC-48, SC-48(1)
		Dynamic Reconfiguration, Functional Relocation of Sensors	Detect	IR-4(2)
		Dynamic Segmentation and Isolation	Shorten, Reduce, Contain, Exert	SC-7(20)
		Mission Dependency and Status Visualization	Detect	SI-4(1)
		Dynamic Privileges	Contain, Exert	AC-2(6)
Endpoint Denial of Service (T1499)	Filter Network Traffic (M1037)	Adaptive Management	Degrade, Reduce	AC-4(3), SC-7(11)
	Maintain Deception Environment (CM1102)	Misdirection	Deceive, Divert	SC-26
		Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Dynamically Restrict Traffic or Isolate Resources (CM1108)	Dynamic Resource Allocation, Adaptive Management	Degrade, Reduce	AU-5(3), IR-4(2), SC-7(20)
	Partition Host (CM1118)	Predefined Segmentation	Degrade, Reduce	SC-2, SC-32
	Monitor Network Usage (CM2047)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Perform Mission Damage Assessment (CM1122)	Mission Dependency and Status Visualization	Detect, Scrutinize	CP-2(8), RA-9
		Sensor Fusion and Analysis, Mission Dependency and Status Visualization	Detect, Scrutinize	SI-4(1)
		Integrity Checks	Detect, Scrutinize	SI-7, SI-7(1)
Firmware Corruption (T1495)	Boot Integrity (M1046)	Integrity Checks	Detect	SI-7, SI-7(9), SI-7(10)
	Privileged Account Management (M1026)	Trust-Based Privilege Management	Negate, Exert	AC-6(5), CM-5(5)
	Switch to Alternate System or Component (CM1143)	Architectural Diversity	Shorten, Reduce	SC-29
		Design Diversity	Shorten, Reduce	SA-17(9)
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	CP-2(5)
	Activate Alternate (CM1144)	Architectural Diversity	Shorten, Reduce, Exert	SC-29
		Design Diversity	Shorten, Reduce, Exert	SA-17(9)
		Specialization	Shorten, Reduce, Exert	SA-20, SA-23
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	CP-2(5)
	Defend Failover and Recovery (CM1145)	Adaptive Management, Dynamic Reconfiguration, Orchestration	Shorten, Reduce, Exert	IR-4(3)
		Functional Relocation of Sensors	Detect	SC-48, SC-48(1)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Dynamic Segmentation and Isolation	Shorten, Reduce, Contain, Exert	SC-7(20)
		Mission Dependency and Status Visualization	Detect	SI-4(1)
		Dynamic Privileges	Contain, Exert	AC-2(6)
	Hardware-Based Protection of Firmware (CM1154)	Integrity Checks	Negate, Preempt	SC-51
Inhibit System Recovery (T1490)	Data Backup (M1053)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Replication	Shorten, Reduce	CP-9(6)
		Protected Backup and Restore, Obfuscation, Integrity Checks	Exert	CP-9(8)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
		Sensor Fusion and Analysis	Detect	SI-4(24)
	Perform Mission Damage Assessment (CM1122)	Mission Dependency and Status Visualization	Detect, Scrutinize	CP-2(8), RA-9
		Sensor Fusion and Analysis, Mission Dependency and Status Visualization	Detect, Scrutinize	SI-4(1)
		Integrity Checks	Detect, Scrutinize	SI-7, SI-7(1)
	Switch to Alternate System or Component (CM1143)	Architectural Diversity	Shorten, Reduce, Exert	SC-29
		Design Diversity	Shorten, Reduce, Exert	SA-17(9)
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	CP-2(5)
	Activate Alternate (CM1144)	Architectural Diversity	Shorten, Reduce, Exert	SC-29

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Design Diversity	Shorten, Reduce, Exert	SA-17(9)
		Specialization	Shorten, Reduce, Exert	SA-20, SA-23
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	CP-2(5)
	Defend Failover and Recovery (CM1145)	Adaptive Management, Dynamic Reconfiguration, Orchestration	Shorten, Reduce, Exert	IR-4(3)
		Functional Relocation of Sensors	Detect	SC-48, SC-48(1)
		Dynamic Reconfiguration, Functional Relocation of Sensors	Detect	IR-4(2)
		Dynamic Segmentation and Isolation	Shorten, Reduce, Contain, Exert	SC-7(20)
		Mission Dependency and Status Visualization	Detect	SI-4(1)
		Dynamic Privileges	Contain, Exert	AC-2(6)
Network Denial of Service (T1498)	Filter Network Traffic (M1037)	Adaptive Management	Degrade, Reduce	AC-4(3)
		Provenance Tracking	Degrade, Reduce	SC-7(11)
	Dynamically Restrict Traffic or Isolate Resources (CM1108)	Dynamic Resource Allocation, Adaptive Management	Degrade, Reduce	AU-5(3), IR-4(2), SC-7(20)
	Monitor Network Usage (CM2047)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
	Switch to Alternate System or Component (CM1143)	Replication	Degrade, Reduce	SC-22
	Defend Against DoS (CM1147)	Dynamic Resource Allocation, Surplus Capacity	Shorten, Reduce	SC-5(2)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
		Monitoring and Damage Assessment	Detect	SC-5(3)
Resource Hijacking (T1496)	Monitor Platform Status (CM2044)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Monitor Network Usage (CM2047)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(11), SI-4(13)
	Dynamically Reprovision (CM1139)	Dynamic Reconfiguration	Shorten	IR-4(2)
		Dynamic Segmentation and Isolation	Reduce	SC-7(20)
	Dynamically Disable or Suspend (CM1121)	Adaptive Management	Preempt, Delay	SC-15(1)
		Dynamic Reconfiguration	Preempt, Delay	AC-2(8)
Service Stop (T1489)	Network Segmentation (M1030)	Predefined Segmentation	Contain, Shorten, Reduce	IR-4(14), SC-3, SC-7(29)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13)
	Monitor Platform Status (CM2044)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Perform Mission Damage Assessment (CM1122)	Mission Dependency and Status Visualization	Detect, Scrutinize	CP-2(8), RA-9
		Sensor Fusion and Analysis, Mission Dependency and Status Visualization	Detect, Scrutinize	SI-4(1)
		Integrity Checks	Detect, Scrutinize	SI-7, SI-7(1)
System Shutdown/Reboot (T1529)	Passive Decoys (CM1104)	Misdirection	Deceive, Detect	SC-26
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Perform Mission Damage Assessment (CM1122)	Mission Dependency and Status Visualization	Detect, Scrutinize	CP-2(8), RA-9
		Sensor Fusion and Analysis, Mission Dependency and Status Visualization	Detect, Scrutinize	SI-4(1)
		Integrity Checks	Detect, Scrutinize	SI-7, SI-7(1)

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
	Switch to Alternate System or Component (CM1143)	Architectural Diversity	Shorten, Reduce, Exert	SC-29
		Design Diversity	Shorten, Reduce, Exert	SA-17(9)
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	CP-2(5)

F.2.4 Candidate Mitigations

Neither a cyber resiliency implementation approach nor a security control *per se* has a potential effect on an adversary TTP or other threat event. Rather, it is the way the cyber resiliency approaches and controls are implemented and used that can produce an effect. In the Potential Effects on Threat Events (PETE) analysis for ATT&CK, descriptions of potential uses of cyber resiliency implementation approaches and controls are captured via ATT&CK mitigations or candidate mitigations. A candidate mitigation is a mitigation, defined in the context of ATT&CK and given an identifier of the form CM####, which has been derived from engineering analysis rather than from a curated data set. It is designated as a "candidate" to differentiate it from the mitigations in the ATT&CK knowledge base. A mitigation or candidate mitigation is given an identifier and a name (a short phrase). These identifiers and names appear in the mapping tables in Section F.2.3.

Tables F-17 through F-19 define the candidate mitigations.[138] The structure of a candidate mitigation is similar to that of mitigations described in the ATT&CK knowledge base (i.e., an identifier, a name, a brief general description, and the cyber resiliency approaches and controls needed to implement the mitigation). The description tailored to individual techniques serves to improve consistency in the analysis of how defender actions or decisions could affect adversary activities as described in ATT&CK. However, because the candidate mitigations are not part of the ATT&CK knowledge base, the identification and numbering scheme is different—that is, candidate mitigation identifiers begin with "CM."

Table F-17 identifies candidate mitigations that are intended to have an effect other than Expose, with identifiers of the form CM11##. Table F-18 identifies candidate mitigations that are solely intended to have the Expose effect, with identifiers of the form CM20##. These candidate mitigations are derived from the Detection descriptions in ATT&CK. Many of the Detection mitigations use the same cyber resiliency controls, particularly IR-4(13) and SI-4(2). However, as indicated by the different names of the candidate mitigations, the implementation of those

[138] See [Bodeau21] for definitions of ATT&CK mitigations.

controls and the use of as-implemented capabilities can vary significantly. Table F-19 identifies candidate mitigations that could increase the effectiveness of other candidate mitigations or ATT&CK mitigations, with identifiers of the form CM13##.[139] Since these candidate mitigations have no direct effect on threat events, they are not included in the PETE analysis for ATT&CK. For each candidate mitigation, one or more cyber resiliency controls (i.e., base controls or control enhancements as listed in Table E-1) are identified, and the cyber resiliency approaches associated with the identified set of controls are also identified. A high-level description of the candidate mitigation is also given.

The controls (and associated cyber resiliency approaches) used by a candidate mitigation to mitigate different threat events can vary. Thus, for a given threat event, only a subset of the controls identified in Tables F-17 through F-19 could be used. In addition, the effects of a mitigation or candidate mitigation on different threat events can vary, depending on the details of the threat events and how the mitigation or candidate mitigation is used.[140]

TABLE F-17: CANDIDATE MITIGATIONS TO REDIRECT, PRECLUDE, IMPEDE, OR LIMIT THREAT EVENTS

Identifier	Name	Description	Cyber Resiliency Approaches	Controls
CM1101	Present Deceptive Information	Present deceptive information about systems, data, processes, and users. Monitor uses or search for presence of that information.	Disinformation, Tainting	SC-30(4), SI-20
CM1102	Maintain Deception Environment	Maintain a distinct subsystem or a set of components specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.	Monitoring and Damage Assessment, Forensic and Behavioral Analysis, Misdirection, Disinformation, Predefined Segmentation	SC-7(21), SC-26, SC-30(4)
CM1103	Detonation Chamber	Use a dynamic execution environment to handle potentially harmful incoming data.	Forensic and Behavioral Analysis, Misdirection, Predefined Segmentation	SC-44
CM1104	Passive Decoys	Use a factitious system or resource to decoy adversary attacks away from operational resources to increase the adversary's workload, or to observe adversary activities.	Misdirection, Architectural Diversity	SC-26, SC-29
CM1105	Component Provenance Validation	Validate the provenance of system components.	Integrity Checks, Provenance Tracking	SR-4, SR-4(1), SR-4(2), SR-4(3), SR-4(4), SR-11
CM1106	Supply Chain Diversity	Provide multiple distinct supply chains for system components.	Supply Chain Diversity	PL-8(2), SR-3(1), SR-3(2)

[139] Gaps in numbering of candidate mitigations are artifacts of the analysis process, and do not indicate that additional candidate mitigations are defined elsewhere.

[140] See [Bodeau21] for descriptions specific to individual ATT&CK techniques.

Identifier	Name	Description	Cyber Resiliency Approaches	Controls
CM1107	Adversarial Simulation	Simulate adversary activities to test the effectiveness of system protections and detection mechanisms.	Self-Challenge	AT-2(1), AT-3(3), CA-8, CA-8(2), SC-7(10), SI-19(8)
CM1108	Dynamically Restrict Traffic or Isolate Resources	Dynamically reconfigure networks to restrict network traffic or isolate resources.	Dynamic Resource Allocation, Adaptive Management, Dynamic Reconfiguration, Dynamic Segmentation and Isolation	AU-5(3), IR-4(2), SC-7(20)
CM1109	Virtual Sandbox	Use virtualization to create a controlled execution environment, which is expunged after execution terminates.	Non-Persistent Services, Dynamic Segmentation and Isolation	SC-7(20), SI-14
CM1110	Application- or Utility-Specific Data Removal	Analyze files and data structures specific to an application or utility for anomalies, and delete them.	Monitoring and Damage Assessment, Integrity Checks, Dynamic Reconfiguration	IR-4(2), IR-4(13), SI-4(2), SI-7(1), SI-7(7)
CM1111	Execution Restriction	Restrict the sources of executables, the locations in which execution can occur, or implement other constraints on execution access.	Attribute-Based Usage Restriction	AC-3(12), AC-3(13)
CM1112	Covert Signaling	Use hidden logic to enable exfiltrated data to signal its location, or embed hidden data that can be the subject of a search.	Tainting	SI-20
CM1113	Present Decoy Data	Present plausible but factitious data assets to attract the adversary. Monitor uses of those assets, or search for the presence of decoy information.	Disinformation, Misdirection, Tainting	SC-26, SC-30(4), SI-20
CM1114	Fragment Information	Fragment information, and distribute it across multiple locations.	Fragmentation	SI-23
CM1115	Lock Down Thin Nodes	Minimize local functionality and disallow writable storage.	Non-Persistent Services, Non-Persistent Information, Restriction, Integrity Checks	SC-25, SC-34, SC-34(1)
CM1116	Dynamic Data Location	Dynamically move data resources.	Functional Relocation of Cyber Resources, Temporal Unpredictability	SC-30(3)
CM1117	Dynamic Account Management	Dynamically update an account's authorizations or privileges.	Dynamic Privileges, Dynamic Reconfiguration	AC-2(6), AC-2(8)

Identifier	Name	Description	Cyber Resiliency Approaches	Controls
CM1118	Partition Host	Partition a host (e.g., server, endpoint system) into separate logical domains.	Predefined Segmentation	SC-2, SC-2(1), SC-32, SC-32(1)
CM1119	Minimize Local Functionality	Construct or configure systems or applications to minimize their inherent functionality.	Restriction	CM-7(2), SC-25
CM1120	Trusted Path	Provide an isolated communications path between the user and security functions.	Predefined Segmentation	SC-11
CM1121	Dynamically Disable or Suspend	Terminate processes or disable capabilities upon triggering conditions.	Adaptive Management, Dynamic Reconfiguration	AC-2(8), SC-15(1)
CM1122	Perform Mission Damage Assessment	Determine the mission consequences of adversary activities (e.g., which resources can be relied on; how quickly, how completely, and with what confidence mission-essential services, data, and communications can be restored from backups or alternative resources).	Sensor Fusion and Analysis, Mission Dependency and Status Visualization, Integrity Checks	CP-2(8), RA-9, SI-4(1), SI-7, SI-7(1)
CM1123	Active Decoys	Use one or more factitious systems or other resources to identify malicious sites, interact with the adversary, actively probe for malicious code, and observe adversary TTPs.	Forensic and Behavioral Analysis, Misdirection, Dynamic Segmentation and Isolation	SC-26, SC-35, SC-44
CM1124	Minimize Data Retention or Lifespan	Minimize the lifespan or retention of data, and ensure that deleted data cannot be retrieved.	Non-Persistent Information, Temporal Unpredictability	SC-23(3), SI-14(2), SI-21
CM1125	Authenticate Devices	Authenticate a device before establishing a connection to it.	Obfuscation, Integrity Checks	IA-3(1)
CM1126	Enhanced Authentication	Use situation-specific, risk-adaptive, or out-of-band authentication.	Adaptive Management, Calibrated Defense-in-Depth, Architectural Diversity, Design Diversity, Path Diversity, Dynamic Privileges	IA-2(13), IA-10, CP-13, SC-47
CM1127	Minimize Duration of Connection or Session	Minimize the time period for which a connection remains open or a session remains active, requiring reauthorization to reestablish connectivity.	Non-Persistent Services, Non-Persistent Connectivity	AC-12, SC-7(10), SC-10, SI-14(3)

Identifier	Name	Description	Cyber Resiliency Approaches	Controls
CM1128	Design Diversity	Use multiple designs to implement the same functionality.	Design Diversity	SA-17(9)
CM1129	Check Policy Consistency	Ensure that policies are applied consistently across systems, applications, and services.	Consistency Analysis	CA-7(5)
CM1130	Validate Data Quality	Validate data quality (e.g., integrity, consistency, correctness).	Integrity Checks	SA-9(7), SI-7(1)
CM1131	Active Deception	Maintain an internal deception environment, divert suspicious traffic to that environment, and interact with and analyze behavior to determine whether it is malicious and to whether investigate adversary TTPs.	Dynamic Reconfiguration, Adaptive Management, Misdirection, Monitoring and Damage Assessment, Forensic and Behavioral Analysis	AC-4(3), IR-4(2), IR-4(3), SC-7(21), SC-26, SC-30(4), SI-3(10)
CM1132	Quarantine or Delete Suspicious Files	Move and make inaccessible or delete suspicious files.	Provenance Tracking, Dynamic Segmentation and Isolation, Non-Persistent Information	SR-4(3), CM-7(6), SI-14, SI-14(2)
CM1133	Isolate or Contain Selected Applications or Components	Isolate or contain (e.g., using internal firewalls or virtual environments) selected applications or components based on risk profiles.	Trust-Based Privilege Management, Predefined Segmentation, Dynamic Segmentation and Isolation	CM-7(6), SC-7(21)
CM1134	Refresh Selected Applications or Components	Refresh software, firmware, or data from a trusted source.	Non-Persistent Services, Non-Persistent Information	SI-14(1), SI-14(2)
CM1135	Hide Sensitive Information	Conceal (e.g., via encryption or data hiding) or remove sensitive information (including metadata).	Obfuscation	SC-28(1), SI-19(4)
CM1136	Identify External Malware	Identify and redirect malware found on external systems.	Monitoring and Damage Assessment, Forensic and Behavioral Analysis, Misdirection, Dynamic Segmentation and Isolation	SC-35
CM1137	Validate Data Properties	Validate data properties (including binaries, metadata, and cryptographic bindings) to defend against modification or fabrication.	Integrity Checks, Calibrated Defense-in-Depth	PL-8(1), SC-16(1), SC-16(3), SI-7, SI-7(1)
CM1138	Switch to Alternative Data Sources	Switch to one or more alternative data sources to ensure adequate data quality or rebuild destroyed data.	Information Diversity, Dynamic Reconfiguration	SI-22, IR-4(2)

Identifier	Name	Description	Cyber Resiliency Approaches	Controls
CM1139	Dynamically Reprovision	Reconfigure or reallocate resources to route around damage.	Adaptive Management, Dynamic Reconfiguration, Dynamic Segmentation and Isolation	AC-4(3), IR-4(2), SC-7(20)
CM1140	Use Alternate Communications	Use alternative communications paths.	Path Diversity	AC-7(4), SC-47
CM1141	Reconstruct Compromised Assets	Reconstruct assets (e.g., files, software components) that have been damaged, destroyed, or modified in a way that makes them suspect.	Information Diversity, Fragmentation, Distributed Functionality, Protected Backup and Restore, Replication, Dynamic Reconfiguration	SC-36, SI-22, SI-23, IR-4(9), CP-9
CM1142	Switch to Protected Hot Shadow	Switch (failover) to a duplicate system in a protected enclave that, subject to additional quality controls on data and software updates, mirrors the system that has been compromised.	Dynamic Reconfiguration, Adaptive Management, Orchestration, Replication, Predefined Segmentation, Integrity Checks	AC-4(2), AC-4(8), CP-2(5), CP-9(6), IR-4(2)
CM1143	Switch to Alternate System or Component	Switch (failover) to another system or system component that provides approximately the same functionality in a different way.	Architectural Diversity, Design Diversity, Dynamic Reconfiguration, Adaptive Management, Orchestration, Replication	CP-2(5), IR-4(2), SA-17(9), SC-22, SC-29
CM1144	Activate Alternate	Activate an alternate system or system component (e.g., from a war-time reserve) that provides approximately the same function in a novel or specialized way, and failover.	Architectural Diversity, Design Diversity, Dynamic Reconfiguration, Adaptive Management, Orchestration, Specialization	CP-2(5), IR-4(2), SA-17(9), SA-20, SA-23, SC-29
CM1145	Defend Failover and Recovery	Increase sensor activity and restrict privileges to defend against an adversary taking advantage of failover or recovery activities.	Adaptive Management, Dynamic Reconfiguration, Orchestration, Functional Relocation of Sensors, Dynamic Segmentation and Isolation, Mission Dependency and Status Visualization, Dynamic Privileges	AC-2(6), IR-4(2), IR-4(3), SC-7(20), SC-48, SC-48(1), SI-4(1)
CM1146	Refresh Sessions or Connections	Terminate and re-establish sessions or network connections unpredictably to disrupt adversary use.	Non-Persistent Connectivity, Temporal Unpredictability	SC-23(3), SC-30(2), SI-14(3)

Identifier	Name	Description	Cyber Resiliency Approaches	Controls
CM1147	Defend Against DoS	Adapt to reduce the impacts of denial-of-service attacks.	Dynamic Resource Allocation, Surplus Capacity, Monitoring and Damage Assessment	SC-5(2), SC-5(3)
CM1148	Conceal or Randomize Network Traffic	Conceal (via encryption or insertion of fabricated traffic) or randomize network traffic patterns.	Obfuscation, Contextual Unpredictability	SC-8(5), SC-30
CM1149	Lock Down Visibility or Access	Restrict the visibility of or access to data based on the nature or attributes of that data.	Attribute-Based Usage Restriction	AC-3(11)
CM1150	Dynamically Relocate and Refresh Processing	Suspend a process and re-instantiate it in a different location.	Functional Relocation of Cyber Resources, Non-Persistent Services	SC-30(3), SI-14(1)
CM1151	Defend Enclave Boundaries	Maintain distinct enclaves based on security characteristics, and use stringent filtering to defend the enclave boundary.	Predefined Segmentation, Integrity Checks, Provenance Tracking	AC-4(8), AC-4(12), AC-4(17), AC-4(21), SC-7(21), SC-7(22), SC-46
CM1152	Defend Against Memory Attacks	Provide defenses against attacks against system memory.	Synthetic Diversity, Temporal Unpredictability	SI-16
CM1153	Modulate Information Flows	Use controlled interfaces and communications paths to provide access to risky capabilities or to filter communications between enclaves.	Orchestration Design Diversity, Replication, Trust-Based Privilege Management, Predefined Segmentation	AC-4(27), AC-4(29), AC-4(30), SC-7(15), SC-46
CM1154	Hardware-Based Protection of Firmware	Use hardware-based protections for firmware.	Integrity Checks	SC-51
CM1155	Validate Output Data	Validate information output from processes or applications against defined criteria.	Integrity Checks	SI-15
CM1156	Physically Relocate Resources	Physically move resources (e.g., storage devices, servers, end-user devices), with concomitant changes to network location.	Asset Mobility	SC-30(3)
CM1157	Defend Against Data Mining	Enforce access restrictions and provide alerting to defend against data mining.	Monitoring and Damage Assessment, Trust-Based Privilege Management, Attribute-Based Usage Restriction, Dynamic Privileges	AC-23

Identifier	Name	Description	Cyber Resiliency Approaches	Controls
CM1158	Defend Audit Data	Provide mechanisms to protect audit data from modification or observation.	Integrity Checks	AU-9(1), AU-9(2), AU-9(3), AU-9(6)
CM1159	Enhance User Preparedness	Keep users, administrators, and operators aware of existing and emerging threats and attack techniques that they can counter in practice.	Dynamic Threat Awareness, Self-Challenge	AT-2(1), AT-2(3), AT-2(5), AT-3(3)
CM1160	Conceal Resources from Discovery	Protect network addresses of system components that are part of managed interfaces from discovery through common tools and techniques, such as hiding or relocation.	Obfuscation, Functional Relocation of Cyber Resources	SC-7(16), SC-30, SC-30(5)
CM1161	Collaborate to Counter Adversaries	Collaborate with other entities to counter adversary activities.	Disinformation, Tainting, Dynamic Threat Awareness	PM-16, SC-30(4), SI-20
CM1162	Restrict Supply Chain Exposures	Limit an adversary's ability to determine or manipulate the organization's cyber supply chain.	Obfuscation, Disinformation, Self-Challenge, Supply Chain Diversity	PM-30(1), SI-4(10), SR-3(2), SR-5, SR-6(1), SR-7, SR-11
CM1163	Redefine System	Redefine the system in terms of components, interfaces, and dependencies.	Orchestration, Architectural Diversity, Supply Chain Diversity, Evolvability, Replication	IR-4(10), SC-27, SC-29, SR-5(1)
CM1164	Calibrate Administrative Access	Configure administrator access to resources based on active defense strategies.	Attribute-Based Usage Restriction, Trust-Based Privilege Management, Restriction	AC-6, AC-6(5), CM-7(2)
CM1165	Physically Relocate Resources	Physically move resources (e.g., storage devices, servers, end-user devices), with concomitant changes to network location.	Asset Mobility	SC-30(3)

TABLE F-18: CANDIDATE MITIGATIONS TO EXPOSE THREAT EVENTS

Identifier	Name	Description	Cyber Resiliency Approaches	Controls
CM2002	Inspect and Analyze Network Traffic	Analyze network traffic for unusual data flows. Traffic inspection and analysis can be performed at the enterprise boundary, at internal boundaries between enclaves, or within enclaves.	Monitoring and Damage Assessment	IR-4(13), SI-4(2), SI-4(4)

Identifier	Name	Description	Cyber Resiliency Approaches	Controls
CM2003	Endpoint Behavior Analysis	Analyze the behavior of endpoint (i.e., end-user, client) systems for anomalous behavior.	Monitoring and Damage Assessment, Behavior Validation	AC-2(12)
CM2004	Monitor Logs	Monitor system and application logs for anomalous or suspicious behavior.	Monitoring and Damage Assessment, Behavior Validation	AU-6, IR-4(13), SI-4(2), SI-4(11)
CM2005	Analyze Logs	Analyze logs (individually or with some correlation across logs) for anomalous or suspicious patterns of behavior.	Monitoring and Damage Assessment, Sensor Fusion and Analysis, Dynamic Resource Analysis, Behavior Validation	AC-2(12), SI-4(13), SI-4(16)
CM2006	Analyze File Contents	Analyze the contents of specific files or types of files for suspicious contents.	Forensic and Behavioral Analysis	SR-10
CM2007	Host Event Detection	Detect anomalous or unauthorized events on hosts (e.g., servers, endpoint systems).	Monitoring and Damage Assessment, Behavior Validation	CM-8(3), IR-4(13), SI-4(2)
CM2008	Removable Device Usage Detection	Detect anomalous or unauthorized events involving the use of removable devices.	Monitoring and Damage Assessment	CM-8(3)
CM2009	Software Integrity Check	Perform integrity checks (e.g., using checksums, hashes, or digital signatures) on software, software certificates, or metadata.	Integrity Checks, Provenance Tracking	SI-7, SI-7(1), SI-7(6), CM-14, SR-4(3)
CM2010	Software Stress Testing	Perform software stress testing (e.g., using out-of-bounds input values) prior to installation.	Self-Challenge	SR-6(1)
CM2011	Physical Inspection	Perform a physical inspection of hardware components for indicators of tampering.	Integrity Checks	SR-9, SR-10
CM2012	Monitor Trusted Parties	Monitor the behavior and status (e.g., change in ownership) of second or third parties.	Dynamic Resource Awareness, Dynamic Threat Awareness, Behavior Validation, Provenance Tracking	PM-16, PM-30(1), SI-4(17)
CM2013	Cross-Enterprise Account Usage Analysis	Analyze user account usage across the enterprise for anomalies or suspicious behavior.	Sensor Fusion and Analysis	AU-6(3), SI-4(16)
CM2014	Process Analysis	Analyze process attributes or behavior for indications of unusual, unauthorized, or suspicious use.	Monitoring and Damage Assessment	IR-4(13), SI-4(2)
CM2015	Process Monitoring	Monitor the behavior of processes for indications of unusual, unauthorized, or suspicious use.	Monitoring and Damage Assessment, Behavior Validation	AU-6, IR-4(13), SI-4(2)

Identifier	Name	Description	Cyber Resiliency Approaches	Controls
CM2016	Cloud Account Monitoring	Monitor activity associated with cloud accounts for indications of unusual, unauthorized, or suspicious use.	Monitoring and Damage Assessment, Behavior Validation	AC-2(12)
CM2017	Privileged Account Monitoring	Monitor and analyze activity associated with privileged accounts for indications of unusual or suspicious use.	Monitoring and Damage Assessment	AC-6(8)
CM2018	Cross-Enterprise Behavior Analysis	Correlate and analyze the behavior of multiple systems.	Sensor Fusion and Analysis	AU-6(3), AU-6(5)
CM2019	Endpoint Scrutiny	Scrutinize the contents and behavior patterns of an endpoint system.	Forensic and Behavioral Analysis	IR-4(12)
CM2020	Application- or Utility-Specific Monitoring	Monitor and analyze events in the context of a specific application or utility.	Monitoring and Damage Assessment, Behavior Validation	IR-4(13), SI-4(2)
CM2021	Account Monitoring	Monitor and analyze activity associated with user accounts for indications of unusual or suspicious use.	Monitoring and Damage Assessment, Behavior Validation	AC-2(12), IR-4(13), SI-4(2)
CM2022	Host-Local Event Correlation	Correlate and analyze events occurring on a single host.	Sensor Fusion and Analysis, Monitoring and Damage Assessment	IR-4(13), SI-4(16)
CM2023	Centralize and Analyze Instance Logging	Centralize instance logging in a cloud or container environment and analyze.	Sensor Fusion and Analysis	AU-6(5), IR-4(4)
CM2029	Monitor Script Execution	Monitor for the execution of scripts that are unknown or used in suspicious ways.	Monitoring and Damage Assessment	IR-4(13), SI-4(2), SI-4(13)
CM2030	Monitor and Analyze API Use	Monitor and analyze uses of application interfaces (APIs).	Monitoring and Damage Assessment	IR-4(13), SI-4(2), SI-4(13)
CM2033	Monitor the File System	Monitor the file system to identify the unexpected presence and atypical use of files of specific types or atypical patterns of access.	Monitoring and Damage Assessment, Sensor Fusion and Analysis, Behavior Validation	IR-4(13), SI-4(2), SI-4(24)
CM2034	Monitor Specific Servers	Monitor specific servers for anomalous or suspicious uses or access attempts.	Monitoring and Damage Assessment	IR-4(13), SI-4(2)
CM2035	Monitor Specific Files	Monitor the use of specific files or directories for anomalous or suspicious uses or access attempts.	Behavior Validation, Monitoring and Damage Assessment	AU-6

Identifier	Name	Description	Cyber Resiliency Approaches	Controls
CM2038	Monitor Command Line Use	Monitor use of the command line interface for common utilities (part of the system or installed by the adversary) and suspicious behavior.	Monitoring and Damage Assessment, Behavior Validation	IR-4(13), SI-4(2), SI-4(4), SI-4(13)
CM2040	Monitor Use of Libraries and Utilities	Monitor the use of libraries and utilities that are commonly used to support adversary actions.	Monitoring and Damage Assessment	IR-4(13), SI-4(2), SI-4(4), SI-4(13)
CM2041	Analyze Network Traffic Content	Analyze the contents of network traffic.	Monitoring and Damage Assessment, Behavior Validation	IR-4(13), SI-4(13), SI-4(25)
CM2042	Analyze Outgoing Traffic Patterns	Analyze outgoing traffic for patterns of behavior that could indicate adversary communications.	Monitoring and Damage Assessment, Behavior Validation	IR4(13), SI-4(18)
CM2043	Monitor External Sources	Monitor and analyze external information sources for indicators of adversary activities, especially those targeting the organization.	Monitoring and Damage Assessment, Dynamic Threat Awareness	PM-16, RA-10
CM2044	Monitor Platform Status	Monitor the status of platforms (e.g., user endpoints, servers, network devices).	Monitoring and Damage Assessment	IR-4(13), SI-4(2)
CM2047	Monitor Network Usage	Monitor network usage for anomalous behavior.	Monitoring and Damage Assessment, Behavior Validation	IR-4(13), SI-4(11), SI-4(13)
CM2048	Hunt for Malicious Processes	Hunt for applications or processes that display specific malicious or suspect behaviors.	Forensic and Behavioral Analysis	IR-5

3175
3176
3177 **TABLE F-19: CANDIDATE MITIGATIONS TO INCREASE THE EFFECTIVENESS OF OTHER MITIGATIONS**

Identifier	Name	Description	Cyber Resiliency Approaches	Controls
CM1301	Dynamic Threat Awareness and Response	Use awareness of the current threat landscape to inform threat hunting and threat-adaptive defenses.	Adaptive Management, Sensor Fusion and Analysis, Dynamic Threat Awareness	RA-3(3), RA-5(10), RA-10, PM-16, PM-16(1)
CM1302	Mission-Oriented Cyber Situational Awareness	Maintain awareness of mission dependencies and the current status of mission-critical assets to inform threat-adaptive responses.	Sensor Fusion and Analysis, Mission Dependency and Status Visualization	SI-4(1), SI-4(2)

Identifier	Name	Description	Cyber Resiliency Approaches	Controls
CM1303	Integrated Non-Disruptive Response	Integrate automated and human-directed response to suspicious events to minimize disruption.	Monitoring and Damage Assessment, Sensor Fusion and Analysis, Adaptive Management	SI-4(3), SI-4(7), SI-7(5)
CM1304	Enhance via Unpredictability	Enhance the effectiveness of defender actions by using capabilities unpredictably or by adding noise or false information to query responses.	Contextual Unpredictability, Temporal Unpredictability	SC-30(2), SI-19(6)
CM1305	Enhance via Heterogeneity	Increase barriers to adversary effectiveness by providing architecturally diverse system components.	Architectural Diversity	AU-9(7), SC-29, SC-29(1)
CM1306	Lock Down Usage	Restrict access to applications and configurations as part of the installation process, and narrowly restrict modifications or other uses of privileged functions.	Attribute-Based Usage Restriction, Trust-Based Privilege Management	AC-3(12), AC-6(10), CM-5(5), CM-5(6), CM-7(4)
CM1307	Enhance via Layered Protections	Provide similar capabilities or mechanisms at multiple architectural layers.	Calibrated Defense-in-Depth	PL-8(1), SC-3(5)
CM1308	Separate Environments with Specific Risks	Provide environments separate from the operational environment for activities with specific risks.	Monitoring and Damage Assessment, Predefined Segmentation	AU-6(8), CM-4(1), SC-7(13)
CM1309	Vulnerability-Oriented Cyber Situational Awareness	Maintain awareness of the vulnerability posture over time to inform the calibration of detection and proactive responses.	Sensor Fusion and Analysis	RA-5(6), RA-5(8), RA-5(10)
CM1310	Protect Distributed Processing and Storage	Provide supporting protections for distributed processing and distributed or replicated storage.	Behavior Validation, Replication	SC-36(1), SC-36(2)
CM1311	Enhance via Isolation	Enhance the effectiveness of or confidence in security functions via system mechanisms for isolation.	Predefined Segmentation, Dynamic Segmentation and Isolation	SC-3(2), SC-39(2), SC-50
CM1312	Enhance Isolation via Hardware Features	Enhance the effectiveness of or confidence in isolation by using underlying hardware features.	Predefined Segmentation, Dynamic Segmentation and Isolation	SC-3(1), SC-39(1), SC-49
CM1313	Validate or Assess Control Effectiveness in Practice	Validate or assess the effectiveness of controls as implemented and used in practice.	Self-Challenge, Protected Backup and Restore, Integrity Checks	CP-4(5), CP-9(1), SI-19(8)

Identifier	Name	Description	Cyber Resiliency Approaches	Controls
CM1314	Enhance via Automation	Use automation to increase the effectiveness or quality of capabilities or practices.	Adaptive Management, Monitoring and Damage Assessment, Sensor Fusion and Analysis, Dynamic Threat Awareness, Integrity Checks, Behavior Validation	CA-7(6) , PE-6(2), PM-16(1), RA-5(6), SI-4(2), SI-4(3), SI-4(7), SI-7(5)
CM1315	Maintain a War-Time Reserve	Maintain a reserve of critical components, both special-purpose and acquired, for use in a crisis situation.	Mission Dependency and Status Visualization, Specialization, Replication	RA-9, SA-20, SA-23, SR-5(1)
CM1316	Enhance via Coordination	Coordinate across the organization and with external stakeholders to increase the effectiveness or timeliness of responsive capabilities and practices.	Adaptive Management, Orchestration	CP-2(1), IR-4(10), IR-4(11)

3178