Draft NIST Special Publication 800-160

VOLUME 2

Systems Security Engineering

Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems

RON ROSS
RICHARD GRAUBART
DEBORAH BODEAU
ROSALIE MCQUAID

This document is a supporting publication to the NIST systems security engineering guidance provided in **Special Publication 800-160, Volume 1**. The content was specifically designed to be used with and to complement the flagship systems security engineering publication to support organizations that require *cyber resiliency* as a property or characteristic of their systems. The goals, objectives, techniques, implementation approaches, and design principles that are described in this publication are an integral part of a cyber resiliency engineering framework and are applied in a life cycle-based systems engineering process.

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

Draft NIST Special Publication 800-160

VOLUME 2

Systems Security Engineering

Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems

RON ROSS
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

March 2018

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by the National Institute of Standards and Technology to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 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 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, Director of OMB, 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, Volume 2
Natl. Inst. Stand. Technol. Spec. Publ. 800-160, Volume 2, **158 pages** (March 2018)
CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts, practices, and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review draft publications during the designated public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at **http://csrc.nist.gov/publications**.

Public comment period: March 21 through May 18, 2018

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

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

Reports on Computer Systems Technology

The NIST Information Technology Laboratory (ITL) promotes the United States 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. 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 and protection of individuals' privacy in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information systems security and its collaborative activities with industry, government, and academic organizations.

Abstract

This publication is intended to be used in conjunction with NIST Special Publication 800-160 Volume 1, *Systems Security Engineering – Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*. 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, allowing the experience and expertise of the organization to determine what is correct for its purpose. Organizations can select, adapt, and use some or all of the cyber resiliency constructs (i.e., goals, objectives, techniques, approaches, and design principles) described in this publication and apply them to the technical, operational, and threat environments for which systems need to be engineered. The system life cycle processes and cyber resiliency constructs can be used for new systems, system upgrades, or repurposed systems; can be employed at any stage of the system life cycle; and can take advantage of any system or software development methodology including, for example, waterfall, spiral, or agile. The processes and associated cyber resiliency constructs 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 protection needs, mission assurance needs, and concerns with cost, schedule, and performance. The tailorable nature of the engineering activities and tasks, and the system life cycle processes, ensure that the systems resulting from the application of the security and cyber resiliency design principles, among others, have the level of trustworthiness deemed sufficient to protect stakeholders from suffering unacceptable losses of their assets and associated consequences. Trustworthiness is made possible in part by the rigorous application of security and cyber resiliency design principles, constructs, and concepts within a structured set of systems life cycle processes that provides the necessary traceability of requirements, transparency, and evidence to support risk-informed decision making and trades.

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; trustworthy.

Acknowledgements

The authors gratefully acknowledge and appreciate the contributions from Jon Boyens, Ed Custeau, Holly Dunlap, Suzanne Hassell, Bill Heinbockel, Daryl Hild, Scott Jackson, Ellen Laderman, Logan Mailloux, Jeff Marron, Cory Ocker, Richard Pietravalle, Victoria Pillitteri, Thom Schoeffling, Matt Scholl, Martin Stanley, Shane Steiger, Mike Thomas, and Beth Wilson, whose thoughtful and constructive 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 and the National Defense Industrial Association (NDIA) Systems Security Engineering Committee for their feedback on the initial drafts of this publication. And finally, a special note of thanks goes to Jim Foti, Elizabeth Lennon, Pat O'Reilly, and Nikki Keller for their outstanding administrative, technical editing, and web support.

Notes to Reviewers

The United States continues to have complete dependence on information technology deployed in critical systems and applications in both the public and private sectors. From the electric grid to voting systems to the vast "Internet of Things" consumer product line, the Nation remains highly vulnerable to sophisticated, cyber-attacks from hostile nation-state actors, criminal and terrorist groups, and rogue individuals. Certain types of advanced threats, known as Advanced Persistent Threats (APTs), have the capability to breach our critical systems, establish a presence within those systems (often undetected), and inflict immediate and long-term damage to the economic and national security interests of the Nation.

For the Nation to survive and flourish in the 21st century where hostile actors in cyberspace are assumed and technology will continue to dominate every aspect of our lives, we must develop trustworthy, secure systems that are cyber resilient. Cyber resilient systems are those systems that have security measures or safeguards "built in" as a foundational part of the architecture and design and moreover, display a high level of resiliency, which means the systems can withstand cyber-attacks, faults, and failures and continue to operate even in a degraded or debilitated state—carrying out the organization's mission-essential functions.

NIST Special Publication 800-160, Volume 2, is the first in a series of specialty publications developed to support *NIST Special Publication 800-160, Volume 1*, the flagship Systems Security Engineering guideline. Volume 2 addresses cyber resiliency considerations for two important, yet distinct communities of interest—

- Engineering organizations developing new systems or upgrading legacy systems employing systems life cycle processes; and
- Organizations with legacy systems as part of their installed base currently carrying out day-to-day missions and business functions.

Both groups can apply the guidance and cyber resiliency considerations to help ensure that the systems that they need, plan to provide, or have already deployed, can survive when confronted by the APT.

It should be noted that the cyber resiliency goals, objectives, techniques, approaches, and design principles described in this publication are not appropriate for every organization, application, or system. Rather, organizations should identify those missions, business functions, and assets that are the most critical and subsequently make appropriate investments in cyber resiliency solutions that support stakeholder needs and concerns.

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.

- **RON ROSS**
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Table of Contents

Prologue

"Among the forces that threaten the United States and its interests are those that blend the lethality and high-tech capabilities of modern weaponry with the power and opportunity of asymmetric tactics such as terrorism and cyber warfare. We are challenged not only by novel employment of conventional weaponry, but also by the hybrid nature of these threats. We have seen their effects on the American homeland. Moreover, we must remember that we face a determined and constantly adapting adversary."

Quadrennial Homeland Security Review Report
February 2010

Foreword

The United States has developed incredibly powerful and complex systems—systems that are inexorably linked to the economic and national security interests of the Nation. The complete dependence on those systems for mission and business success in both the public and private sectors, including the critical infrastructure, has left the Nation extremely vulnerable to hostile cyber-attacks and other serious threats, including natural disasters, structural/component failures, and errors of omission and commission. The susceptibility to such threats was described in the January 2013 Defense Science Board Task Force Report entitled *Resilient Military Systems and the Advanced Cyber Threat*. The reported concluded that—

> "*…the cyber threat is serious and that the United States cannot be confident that our critical Information Technology systems will work under attack from a sophisticated and well-resourced opponent utilizing cyber capabilities in combination with all of their military and intelligence capabilities (a full spectrum adversary) …*"

The Defense Science Board Task Force stated that the susceptibility to the advanced cyber threat by the Department of Defense is also a concern for public and private networks, in general, and recommended that steps be taken immediately to build an effective response to measurably increase confidence in the systems we depend on (in the public and private sectors) and at the same time, decrease a would-be attacker's confidence in the effectiveness of their capabilities to compromise those systems. This conclusion was based on the following facts:

- The success adversaries have had in penetrating our critical systems and networks;
- The relative ease that our Red Teams have in disrupting, or completely defeating, our forces in exercises using exploits available on the Internet; and
- The weak security posture of our systems and networks.

The Task Force also described several tiers of vulnerabilities within organizations including known vulnerabilities, unknown vulnerabilities, and adversary-created vulnerabilities. The important and sobering message is that the top two tiers of vulnerabilities (i.e., the unknown vulnerabilities and adversary-created vulnerabilities) are, for the most part, totally invisible to most organizations. These vulnerabilities can be effectively addressed by sound systems security engineering approaches—in essence, providing the necessary trustworthiness to withstand and survive well-resourced, sophisticated cyber-attacks on the systems supporting critical missions and business operations.

To begin to address the challenges of the 21st century, we must:

- Understand the modern threat space (i.e., adversary capabilities and intentions revealed by the targeting actions of those adversaries);
- Identify stakeholder assets and protection needs and provide protection commensurate with the criticality of those assets and needs and the consequences of asset loss;
- Increase the understanding of the growing complexity of systems—to more effectively reason about, manage, and address the uncertainty associated with that complexity;
- Integrate security requirements, functions, and services into the mainstream management and technical processes within the system development life cycle; and
- Prioritize, design, and build trustworthy secure systems capable of protecting stakeholder assets.

SYSTEM SECURITY AS A 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 publication addresses the engineering-driven actions necessary to develop more defensible and survivable systems—including other systems that depend on those systems. It starts a set of well-established International Standards for systems engineering published by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the Institute of Electrical and Electronics Engineers (IEEE), and infuses systems security engineering approaches into those systems. The aim of the NIST Systems Security Engineering initiative is to address security, safety, and resiliency issues from a stakeholder requirements and protection needs perspective and to use established engineering processes to ensure that such requirements and needs are addressed with the appropriate fidelity and rigor across the entire system development life cycle.

In addition to the systems engineering community, this publication can also serve the needs of organizations responsible for acquiring, managing the project for acquiring, and using systems to support essential missions and functions. As such, references to risk management and risk management strategies can have two legitimate interpretations—managing the risk associated with developing a system (i.e., project-related, systems engineering viewpoint); or managing the security and privacy risks associated with requirements arising from legislation, regulations, policies, standards, or the organization's mission or business activities. The cyber resiliency engineering framework is sufficiently flexible to be able to support both communities by tailoring and applying the content appropriately to either an engineering-focused systems life cycle process or to an installed base of legacy systems as part of an enterprise-wide information security or privacy program.

Increasing the trustworthiness of systems is a significant undertaking that requires a substantial investment in the requirements, architecture, design, and development of systems, components, applications, and networks—and a fundamental cultural change to the current "business as usual" approach. Introducing a disciplined, structured, and standards-based set of systems security engineering activities and tasks provides an important starting point and forcing function to initiate needed change. The ultimate objective is to obtain trustworthy secure systems that are fully capable of supporting critical missions and business operations while protecting stakeholder assets, and to do so with a level of assurance that is consistent with the risk tolerance of those stakeholders.

-- Ron Ross

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

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 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 reprinted with permission from the Institute of Electrical and Electronics Engineers and is noted as follows:

HOW TO USE THIS PUBLICATION

This publication is intended to be used in conjunction with NIST Special Publication 800-160 Volume 1, *Systems Security Engineering – Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*. Like Volume 1, this publication 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, it can be viewed as a catalog or handbook for achieving the identified cyber resiliency outcomes of a systems 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 (goals, objectives, techniques, approaches, and design principles) described in this publication and tailor them as appropriate 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 **ISO/IEC/IEEE 15288** processes and some or all of the security-related activities and tasks defined for each process. Note that there are process dependencies, and the successful completion of some activities and tasks necessarily 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; can be employed at any stage of the system life cycle; and can take advantage of any system and/or software development methodology including, for example, waterfall, spiral, or agile. The 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 will ensure that the specific systems resulting from the application of the security design principles and concepts have the level of trustworthiness deemed sufficient to protect stakeholders from suffering unacceptable losses of their 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 disciplined and structured set of processes that provides the necessary evidence and transparency to support risk-informed decision making and trades.

GETTING THE MAXIMUM BENEFIT FROM THIS PUBLICATION

This publication is ***not*** intended to formally define Systems Security Engineering (SSE); make a definitive or authoritative statement of what SSE is and what it is not; define or prescribe a specific process; or prescribe a mandatory set of activities for compliance purposes. This publication ***is*** intended to address the activities and tasks, the concepts and principles, and most importantly, what should be "considered" from a cyber resiliency perspective when executing within the context of Systems Engineering (hence the alignment to the international standard **ISO/IEC/IEEE 15288**) as described in Volume 1: *Systems Security Engineering – Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*.

- The use of the term "considerations" is intended to emphasize that this publication is not claiming to be "the" answer for the formal statement of SSE and all forms of its application to achieve resiliency in software-intensive and cyber-enabled systems. It does not define SSE, but offers considerations towards what can and should be done now and from which there can be continued evolution and maturation towards more effective and *context–sensitive* application of the considerations to address the breadth and depth of system security and cyber resiliency problems. In that regard, the document is not "a process" but a collection of related processes, where each process addresses an aspect of the system security problem space and offers a cohesive set of activities, tasks, and outcomes that combine to achieve the end goal of a trustworthy secure system. The application of any process must be properly calibrated to the objectives and constraints in the *context* to which the process is applied—and conducted with an appropriate level of rigor.
- The use of the term "in the engineering of" is intended to emphasize that the focus is on engineering (as opposed to operating). The objective of the publication is to be engineering-based, not operations- or technology-based. Considerations are grounded in a systems engineering viewpoint of system life cycle processes. Organizations using the publication will certainly tailor the system life cycle processes for effectiveness, feasibility, and practicality, but in doing so they have the responsibility to achieve the stakeholder's stated outcomes nonetheless. There can be legitimate variances with the activities and tasks and how they are accomplished, or whether they have value in the context of their application. These variances occur when differing and sometimes conflicting views must be addressed and traded among to achieve the combined objectives of all stakeholders in a cost-effective manner.

Note: *Context-sensitive* cyber resiliency means that stakeholders establish the relative priorities of their cyber resiliency goals and objectives and the context to subsequently apply the appropriate SSE activities and tasks that provide a level of cyber resiliency that falls within their tolerance of loss and associated risk. Context-sensitive application of the SSE activities and tasks in this publication is precisely what systems engineering expects. With sufficient understanding of SSE, the context-sensitive application happens as a natural by-product of systems engineering. It is essential that the processes be adaptable and tailorable to address the *complexity* and *dynamicity* of all factors that define the system and its environmental context. This includes the system-of-systems environment where such systems may not have a single owner, may not be under a single authority, or may not operate within a single set of priorities. The system-of-systems context potentially requires the execution of these processes along a different line of reasoning. The fundamentals and concepts of SSE are still applicable, but may have to be applied differently. This is one of the primary objectives for the *Systems Security Engineering Framework* and the associated SSE activities and tasks provided in this publication.

NIST SYSTEMS SECURITY ENGINEERING INITIATIVE

NIST Special Publication 800-160, Volume 1 is the flagship publication in a series of planned systems security engineering publications. The series of 800-160 publications will include several important systems security engineering topics, for example: *hardware security and assurance*; *software security and assurance*; and *system resiliency*. Each topic will be addressed in the context of the system life cycle processes contained in **ISO/IEC/IEEE 15288** and the security-related activities and tasks that are described in Special Publication 800-160, Volume 1.

NIST plans to update its foundational security and risk management guidance to describe how such guidance might be interpreted and applied at the enterprise level and in association with systems engineering processes.

Errata

This table contains changes that have been incorporated into NIST Special Publication 800-160, Volume 2. Errata updates can include corrections, clarifications, or other minor changes in the publication that are either *editorial* or *substantive* in nature.

DATE	TYPE	REVISION	PAGE

CHAPTER ONE

INTRODUCTION

THE NEED FOR CYBER RESILIENT SYSTEMS

The need for trustworthy secure *systems*[1] 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 800-160, Vol.1] provides guidance on systems security engineering with an emphasis on protection against *asset* loss.[2] In addition to security, other aspects of trustworthiness include, for example, reliability, safety, resilience, and privacy. Specialty engineering disciplines address different aspects of trustworthiness. While each specialty discipline frames the problem domain and the potential solution space for its aspect of trustworthiness somewhat differently, [NIST 800-160, Vol. 1] 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*.[3]

NIST Special Publication 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 regardless of the source.[4] Cyber resiliency supports mission assurance in a contested environment, for missions which 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. A cyber resource which can be accessed via a network exists in or has a presence in cyberspace. However, some information resources are 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 stand-off mode.[5]

---

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

[2] 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 [NIST 800-160, Vol. 1] for the system security perspective on assets.

[3] A *system-of-interest* is a system whose life cycle is under consideration in the context of [ISO/IEC/IEEE 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.

[4] 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 [NIST 800-160, Vol. 1] 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.

[5] 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 purposes of cyber resiliency engineering analysis.

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 domain is thus defined as the problem of achieving adequate mission resilience by providing adequate *system resilience*[6] in the presence of possible adversity affecting cyber resources. The cyber resiliency problem domain overlaps with the security problem domain, since a system should be securely resilient.[7] The cyber resiliency problem domain is guided and informed by an understanding of the threat landscape and in particular, the advanced persistent threat (APT).[8] A *cyber resilient system* is a system that provides a degree of cyber resiliency commensurate with the system's importance or criticality, treating cyber resiliency as one aspect of trustworthiness which requires assurance in conjunction with other aspects such as security, reliability, privacy, and safety.

1.1 PURPOSE AND APPLICABILITY

The purpose of this document is to supplement NIST Special Publication 800-160, Volume 1 with guidance on how to apply cyber resiliency concepts, constructs, and engineering practices, as part of systems security engineering. This document identifies considerations towards the engineering of systems of the following types, which are not mutually exclusive:

- **New Systems**

  The engineering effort includes such activities as concept exploration, analysis of alternative solutions, and preliminary or applied research to refine the concepts and/or feasibility of technologies employed in a new system. This effort is initiated during the concept and development stages of the system life cycle. The engineering effort takes into consideration the full range of possible adversity, seeks synergies between cyber resiliency and other aspects of trustworthiness, and provides the broadest scope for defining, analyzing, and implementing cyber resiliency solutions.

- **Modifications to Systems**

  Reactive modifications to fielded systems: The engineering effort occurs in response to adversity in the form of disruptions, hazards, and threats such as cyber-attacks, incidents, errors, accidents, faults, component failures, and natural disasters that diminish or prevent the system from achieving its desired capability. Such adversity increases stakeholder awareness of and concerns for cyber resiliency. This effort provides opportunities for introducing cyber resiliency solutions into the system (including its hardware, firmware, and software system elements and operational processes). Such opportunities are constrained by considerations of cost and potential impact on mission or business functionality. This effort can occur during the production, utilization, or support stages of the system life cycle and may be performed concurrently with or independent of day-to-day operations.

---

[6] *System resilience* is defined by the INCOSE Resilient Systems Working Group 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]."

[7] The term *securely resilient* refers to the system's ability to preserve a secure state despite disruption, to include the system transitions between normal and degraded modes. System resiliency is a primary objective of systems security engineering [NIST 800-160 Vol. 1].

[8] The Advanced Persistent Threat (APT) is 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 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 [NIST 800-39].

Planned upgrades to fielded systems while continuing to sustain day-to-day operations: The planned system upgrades may enhance an existing system capability, provide a new capability, or constitute a technology refresh of an existing capability. This effort also provides constrained opportunities for introducing cyber resiliency solutions into the system. This effort occurs primarily during the utilization or support stages of the system life cycle.

Planned upgrades to fielded systems that result in new systems: The engineering effort is carried out as if developing a new system with a system life cycle that is distinct from the life cycle of a fielded system. This effort provides opportunities for introducing cyber resiliency solutions into the system. Since the upgrades are performed in a development environment that is independent of the fielded system, greater scope is afforded in defining, analyzing, and implementing cyber resiliency solutions.

- **Dedicated or Special-Purpose Systems**

  Security-dedicated or security-purposed systems: The engineering effort delivers a securely resilient, security-dedicated, or security-purposed system. Such systems can include shared security services (e.g., identity and access management services), surveillance systems, monitoring systems, and security service provisioning systems.

  Cyber-physical systems (CPS):[9] The engineering effort delivers a system in which the interactions within the cyber domain and between the cyber and physical domains do not undermine system resilience, security, or safety. Such systems may include multiple operational states or modes with varying forms of manual, semi-manual, or autonomous modes, and may be capable of operating in a stand-off mode (i.e., without a network connection).

  High-confidence, dedicated-purpose systems: The engineering effort delivers a system that satisfies the need for real-time control of vehicles, industrial or utility processes, weapons, nuclear, or other special-purpose needs. Such control systems are CPS or may include CPS system elements. These systems have highly deterministic properties, strict timing constraints and functional interlocks, and severe if not catastrophic consequences of failure.

  Large-scale processing environments (LSPE): The engineering effort delivers a system which enables large numbers of events to be handled (e.g., transactions to be processed) with high confidence in service delivery. The scale of such systems makes them highly sensitive to disruptions in or degradation of service.

- **General-Purpose or Multi-Use Systems**

  Enterprise information technology (EIT): The engineering effort delivers assured information resources which can meet the mission or business needs of an enterprise.

  Shared services and common infrastructures: The engineering effort delivers a system which can meet the needs of its stakeholder community (whether internal to an enterprise or drawn from multiple organizations), typically as expressed via service-level agreements (SLAs). Such systems are natural targets for malicious cyber activity, since they provide a stepping stone to the systems, missions, and user communities they serve.

- **System-of-Systems**

  The engineering effort occurs across a set of constituent systems, each system with its own stakeholders, primary purpose, and planned evolution. The composition of the constituent

[9] 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 [NIST 1500-201].

systems into a *system-of-systems* [Maier98] produces a capability that would otherwise be difficult or impractical to achieve. This effort can occur across a continuum of system-of-systems types from a relatively informal, unplanned system-of-systems concept and evolution that emerges over time via voluntary participation, to degrees of more formal execution with the most formal being a system-of-systems concept that is directed, planned, structured, and achieved via a centrally managed engineering effort. This effort includes the analysis of the dependencies and interactions among constituent systems and system elements which could enhance cyber resiliency (e.g., by providing diversity in conjunction with redundancy or by enabling functionality to be reconstituted from a different set of resources than were initially used to provide the functionality). This effort also includes analysis of how dependencies and interactions among constituent systems and system elements could be exploited by threats, or could lead to cascading failures.

- **Critical Infrastructure Systems (CIS)**

  The engineering effort addresses concerns related to CPS, high-confidence dedicated-purpose systems, and LSPE. In addition, the engineering effort takes into consideration issues of risk governance, regulations, and standards of good practice specific to the critical infrastructure sector, and system-of-systems concerns for cascading failures and use of low-value systems as stepping stones for attack activities.

- **Evolution of Systems**

  The engineering effort involves migrating or adapting a system or system implementation from one operational environment or set of operating conditions to another operational environment or other set of operating conditions. This effort explicitly considers the cyber resiliency goal of adaptation in the face of changing forms of adversity, as well as changes to the operational environment and technological evolution. This also considers the introduction of vulnerabilities during evolution and the need to maintain resiliency while the system is in intermediate or transition points between evolutionary forms.

- **Retirement of Systems**

  The engineering effort removes system functions or services and associated system elements from operation, to include removal of the entire system, and may also include the transition of system functions and services to some other system. The effort occurs during the retirement stage of the system life cycle and may be carried out while sustaining day-to-day operations. The effort considers the consequences of retirement activities on the cyber resiliency of other systems, including those systems which depend on or interact with the system-of-interest and those systems to which system functions and services are transitioned. This also considers the vulnerabilities that may inadvertently be introduced by the unintended existence of residual elements persisting after retirement.

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 [NIST 800-160, Vol. 1].[10] The term *systems security engineer* is used to include those security professionals

[10] This includes security, privacy, and risk management practitioners with significant responsibilities for the protection of legacy systems, information, and the information technology infrastructure within enterprises (i.e., 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 the use of the *Risk Management Framework* [NIST 800-37], the security and privacy controls in [NIST 800-53], or the *Framework for Improving Critical Infrastructure Cybersecurity* [NIST CSF] where such applications have cyber resiliency-related concerns.

who perform any of the activities and tasks in Special Publication 800-160. It may apply to an individual or a team of individuals from the same organization or different organizations. This publication can also be used by professionals who perform other system life cycle activities 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;
- 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; and
- Academic institutions offering systems security engineering and related programs.

1.3 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** provides background information on the fundamental concepts associated with cyber resiliency; a description of the conceptual framework for cyber resiliency engineering; and general considerations for applying cyber resiliency.
- **Chapter Three** describes the application of cyber resiliency to systems engineering processes.
- Supporting appendices provide additional cyber resiliency-related information including:
  - **Appendix A** (References);
  - **Appendix B** (Glossary);
  - **Appendix C** (Acronyms);
  - **Appendix D** (Cyber Resiliency Techniques);
  - **Appendix E** (Implementation Approaches);
  - **Appendix F** (Design Principles);
  - **Appendix G** (Controls Supporting Cyber Resiliency);
  - **Appendix H** (Relationships Among Cyber Resiliency Constructs);
  - **Appendix I** (Cyber Resiliency Effects on Adversary Activities); and
  - **Appendix J** (Mitigating Advance Persistent Threats).

SYSTEM RESILIENCE AND CYBER RESILIENCY

COMPARING AND CONTRASTING

An automobile contains many cyber resources including, for example, embedded control units for acceleration, braking, and engine control; and entertainment and cellular communications systems. The automobile and its human operator can be viewed as a *system-of-interest* from the systems security engineering standpoint. The system-of-interest has an assumed environment of operation (including, for example, a set of 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* considers whether and how easily the operator could fail to notice a low-fuel or low-battery indicator; a system resilience engineering analysis also 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* 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. This document focuses on cyber resiliency, as an emerging specialty systems engineering discipline, applied in conjunction with resilience engineering and systems security engineering.

CHAPTER TWO

THE FUNDAMENTALS

BASIC CONCEPTS ASSOCIATED WITH CYBER RESILIENCY

This section presents a broad overview and background information on cyber resiliency; a conceptual framework for understanding and applying the concepts of cyber resiliency; a concept of use for the conceptual framework; and specific engineering considerations for implementing cyber resiliency in the system life cycle. 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. The *constructs* are the basic elements of the conceptual framework and include goals, objectives, techniques, implementation approaches, and design principles.[11] The framework provides a way to understand the cyber resiliency problem and solution domain. Goals and objectives identify the "what" of cyber resiliency. The techniques, approaches, and design principles characterize ways of achieving or improving resilience in the face of threats to systems and system components (i.e., the "how" of cyber resiliency). While this characterization includes threats from cyber and non-cyber sources as well as adversarial and non-adversarial threats, the concern for cyber resiliency focuses on aspects of trustworthiness—in particular, security and resilience—and risk from the vantage point of mission assurance against the determined adversaries.

> **"This whole economic boom in cybersecurity seems largely to be a consequence of poor engineering."**
> -- Carl Landwehr, *Communications of the ACM,* February 2015

Cyber resiliency *engineering practices* are the methods, processes, modeling and analytic 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/IEC/IEEE 15288, and NIST 800-160 Vol. 1]. Such solutions include combinations of technologies, architectural decisions, systems engineering processes, and operational policies, processes, procedures, or practices which solve problems in the cyber resiliency domain—that is, they provide a sufficient level of cyber resiliency to meet stakeholder needs and to reduce risks to 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 3.1.3. Cyber resiliency solutions apply design principles, as described in Section 3.1.4. Cyber resiliency solutions typically implement mechanisms (e.g., security and privacy controls and control enhancements as defined in [NIST 800-53]) which require the use of one or more cyber resiliency techniques or approaches, or which are intended to achieve one or more cyber resiliency objectives. The mechanisms are selected in response to the security and cyber resiliency requirements defined as part of the system life cycle requirements engineering process described in [NIST 800-160, Vol. 1], or to mitigate security and cyber resiliency risks that arise from architectural or design decisions due to trade-offs.

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

2.1 BACKGROUND

This section provides background information on cyber resiliency. It defines cyber resiliency in the context of systems that include cyber resources; describes the distinguishing characteristics of cyber resiliency including the assumptions which underpin this specialty engineering discipline; defines the relationship between cyber resiliency and other specialty engineering disciplines; and describes the relationship between cyber resiliency and risk.

2.1.1 DEFINING CYBER RESILIENCY

Cyber resiliency[12] is defined in this publication 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 system; to a mechanism, component, or system element; to a shared service, common infrastructure, or system-of-systems identified with a mission or business function; to an organization;[13] to a critical infrastructure sector or a region; to a system-of-systems in a critical infrastructure sector or sub-sector; and to 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:

- **Resilience for the Nation:** The ability to *adapt* to changing conditions and *prepare* for, *withstand*, and rapidly *recover* from disruption [PPD-8].
- **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].
- **Community Resilience:** The ability of a community to *prepare* for anticipated hazards, *adapt* to changing conditions, *withstand* and *recover* rapidly from disruptions [NIST 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 [PPD-21].
- **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 [NIST 800-53].

[12] "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 was simply resilience engineering with "cyber" as a modifier. The term "cyber resilience" is being used by many organizations today to refer to organizational resilience against cyber threats, with a strong emphasis on effective implementation of good cybersecurity practices and continuity of operations (COOP). For example, the DHS Cyber Resilience Review (CRR), which is based on the 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" generally omit the architecture and engineering aspect, which is the focus of the cyber resiliency engineering framework and of the design principles discussed in this publication.

[13] See [NIST 800-39] for a discussion of the system, mission/business function, and organization levels. See the NIST Cybersecurity Framework [NIST CSF] for a discussion of the system-of-systems and critical infrastructure levels.

- **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 [DOD 8140.01].
- **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 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.

2.1.2 DISTINGUISHING CHARACTERISTICS OF CYBER RESILIENCY ENGINEERING

Cyber resiliency engineering differs from other disciplines in terms of its focus and threat assumptions. These are reflected in cyber resiliency constructs and engineering practices.

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

  Cyber resiliency focuses on capabilities supporting organizational missions or business functions. It maximizes the ability of organizations to complete critical or essential missions or business functions despite an adversary presence in their systems and infrastructure, threatening mission-critical systems and system components. While organizations make their systems and components resilient, this is done to support mission and business assurance. In some cases, system components that are less critical to mission or business effectiveness are sacrificed to contain a cyber-attack and maximize mission assurance.

- **Focus on the effects of the Advanced Persistent Threat.**

  Cyber resiliency addresses all threats to systems containing cyber resources, whether such threats are cyber or non-cyber (e.g., kinetic) in nature. But the focus of cyber resiliency is on the APT. 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, APT actors can take advantage of or make their 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 which 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 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 most modern systems are large and complex entities, and as such, there will always be weaknesses and flaws in the systems, operational environments, and supply chains that adversaries will be

able to exploit. As a result, a sophisticated adversary can penetrate an organizational system and achieve a presence within a targeted organization's infrastructure.

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

  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 mitigations that previously were successful may no longer be effective. And finally, cyber resiliency 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 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.

ADVERSARY PERSISTENCE AND LONG-TERM PRESENCE

The following examples illustrate the types of situations where an adversary can maintain a long-term presence or persistence in a system—

- 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, code repositories, continuous integration tools). 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]).

2.1.3 RELATIONSHIPS WITH OTHER SPECIALTY ENGINEERING DISCIPLINES

Cyber resiliency is an aspect of trustworthiness, as are safety, system resilience, survivability, reliability, security and privacy.[14] Cyber resiliency concepts and engineering practices assume a foundation of security and reliability; many cyber resiliency techniques use or rely on security, reliability, and resilience mechanisms. 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" [NIST 800-82]. Safety engineering focuses on identifying unacceptable system behaviors, outcomes, and interactions, and on ensuring that the system does not enter an unacceptable state (i.e., one in which such behaviors, interactions, or outcomes are possible, thus creating or being an

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

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.

[NIST 800-160 Vol. 1] 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 (See Section 2.2.2), a system may need to operate transiently in an unsafe (or an insecure) state, depending on how stakeholders prioritize and trade off required system properties.

- **Security**

  Cyber resiliency engineering may be viewed as a specialty discipline of systems security engineering. [NIST 800-160 Vol. 1] defines security as "freedom from those conditions that can cause loss of assets with unacceptable consequences."[15] Therefore, security is concerned with the protection of assets, and is primarily oriented to the concept of asset loss.[16] Cyber resiliency 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 focuses on capabilities supporting missions or business functions, and on the effects of adversarial actions on systems.

  While [NIST 800-160 Vol. 1] 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].[17] Cyber resiliency engineering considers a broader range of cyber effects than the loss of confidentiality, integrity, or availability of information. Cyber effects of concern include the effects of concern to security, including service degradation and denial or interruption of service; non-disruptive modification or fabrication as well as 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 finally, alterations in behaviors affecting 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 (discussed in Section 2.2.3) rely on the correct and effective application of security controls. Some cyber resiliency design principles (discussed in Section 2.2.4) adapt or are strongly aligned with the security design principles described in [NIST 800-160 Vol. 1].

---

[15] It is noted that this is a broader construction than 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.

[16] 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 encompasses avoiding asset loss and consequences; detecting asset loss and consequences; minimizing (i.e., limiting, containing, or 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 [NIST 800-160 Vol. 1].

[17] Note that Appendix G.3.1 of [NIST 800-160 Vol. 1] adapts these security objectives to be more broadly applicable.

- **Resilience and Survivability**

  The specialty disciplines of resilience engineering and survivability engineering address system resilience, independent of whether the system-of-interest contains cyber resources. Cyber resiliency assumes 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, and recover from disruptions by restoring the pre-disruption state as closely as possible" [Madni07, Madni09].

  Survivability engineering "is the subset of systems engineering concerned with minimizing the impact of environmental disturbances on system performance. Survivability may be 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 draws numerous concepts and design principles from resilience engineering and survivability engineering. However, the risk model for cyber resiliency differs from that typically used in these specialty engineering disciplines. Concepts and design principles for survivability and resilience are adapted or extended to reflect the concerns for the APT.

- **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 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.

- **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" [NIST 800-82]. Classes of faults include development faults, physical faults, and interaction faults. Faults can be characterized by phase of creation or occurrence—whether they are internal or external to a system, whether they are natural or human-made, whether they are in hardware or software, persistence, and properties related to human-made faults [Avizienis04]. An advanced adversary can cause, emulate, or take advantage of a fault. Cyber resiliency draws some techniques or implementation approaches (See Section 2.2.3) from fault tolerance, and can leverage capabilities motivated by fault tolerance, while assuming that the actions of an advanced adversary may go undetected.

- **Privacy**

  Privacy protection should be accorded to the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of personally identifiable information (PII). Privacy engineering is characterized as "a specialty discipline of systems engineering focused on achieving freedom from conditions that can create problems for individuals with unacceptable consequences that arise from the system as it processes PII" [NISTIR 8062]. Cyber resiliency relates to privacy to the extent that privacy protection is a stakeholder requirement.

2.1.4 RELATIONSHIP BETWEEN CYBER RESILIENCY AND RISK

Cyber resiliency solutions are intended to reduce the risk of depending on systems containing cyber resources, primarily by reducing the extent of harm from threat events,[18] but also by reducing the likelihood of occurrence of threat events and the likelihood the threat events will cause harm.[19] The risk model for cyber resiliency identifies the specific 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, resilience engineering, and survivability. However, the cyber resiliency risk model focuses on 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, but focuses on the APT. Sophisticated adversaries can use tactics, techniques, and procedures (TTPs) typical of less sophisticated threat actors, can take advantage of threat events due to such sources as natural disaster or infrastructure failure, and can imitate or leverage human error or loss of component reliability. These adversaries execute cyber campaigns that can involve multiple systems and organizations, and can extend for periods of months or even years.[20]

The *consequence model* for cyber resiliency encompasses consequences to information and to 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; exfiltrated or exposed information; or usurped or misused system resources. However, the consequence model for cyber resiliency also considers 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). In general, a cyber resiliency solution identified for a given scope is intended to reduce risks at the next level, prioritized by capability. This is illustrated in Table 1.

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

[19] While many different risk models are potentially valid and useful, three elements are common across most models. These are: 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); 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 the *level of the impact* [NIST 800-30].

[20] Activities and threat events can be drawn from [NIST 800-30], with augmentation or additional detail from other sources; the stages or phases of a cyber-attack can be drawn from NIST or from the Office of the Director of National Intelligence (ODNI) *Cyber Threat Framework* [ODNI17].

TABLE 1: CYBER RESILIENCY SOLUTIONS MITIGATE RISK AT A BROADER SCOPE

SCOPE OF SOLUTION	SCOPE OF RISKS TO BE MITIGATED
System element	System
System	Mission or business function, shared service, common infrastructure, or system-of-systems within an organization
Mission or business function, shared service, common infrastructure, or organization-internal system-of-systems identified with a mission or business function	Organization, organizational stakeholders, owners or operators of constituent systems within the organization which rely on the shared service or common infrastructure
Organization	Stakeholders in organizational mission or business function (e.g., customers, partners, suppliers, other organizations in the same critical infrastructure sector or sub-sector as the organization) or in organizational operations (e.g., individuals whose PII the organization handles)
Multi-organization system-of-systems (e.g., value chain in a critical infrastructure sector or sub-sector)	Customers, partners, suppliers, other groups of individuals or organizations, or region dependent on the value provided by the system-of-system

Consequences to a mission or business function, or to an organization, can be defined in terms of impacts on 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 system models which represent quality properties.[21]

Security. The threat model for cyber resiliency encompasses the security threat model, but emphasizes the APT. The consequence model differs in that it treats loss of system assets as instrumental to consequences at a broader scope. Thus, it requires systems engineers analyzing risks to view the system-of-interest not only in terms of how its environment of operation[22] imposes constraints but also how adversity involving cyber resources and consequently the system-of-interest affect that environment.

Resilience and survivability. The threat model for resilience engineering and for survivability focuses on an event or a set of circumstances which disrupts normal 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: such adversary-caused harms as fabrication of user accounts or 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). The consequence model for cyber resiliency encompasses the consequence model for resilience and survivability.

[21] *Quality properties* are emergent properties of systems that include, for example: safety, security, maintainability, resilience, reliability, availability, agility, and survivability [NIST 800-160, Vol. 1]. These properties are also referred to as *systemic properties* across many engineering domains.

[22] See Figure 2 in [NIST 800-160 Vol. 1].

2.2 CYBER RESILIENCY ENGINEERING FRAMEWORK

The following sections provide a description of the conceptual framework for cyber resiliency engineering.[23] The framework constructs include cyber resiliency goals, objectives, techniques, approaches, and design principles. The relationship among constructs is also described.

2.2.1 CYBER RESILIENCY GOALS

As noted in Section 2.1.1, four high-level goals are common to many resiliency definitions, and are reflected in the definition of cyber resiliency. Cyber resiliency goals help to scope the cyber resiliency domain. The term *adversity*, as used in the cyber resiliency goals in Table 2, specifically includes stealthy, persistent, and sophisticated adversaries, who may have already compromised system components and established a foothold within an organization's systems.

TABLE 2: CYBER RESILIENCY GOALS

GOAL	DESCRIPTION
Anticipate	Maintain a state of informed preparedness for adversity.
Withstand	Continue essential mission or business functions despite adversity.
Recover	Restore mission or business functions during and after adversity.
Adapt	Modify mission or business functions and/or supporting capabilities to predicted changes in the technical, operational, or threat environments.

2.2.2 CYBER RESILIENCY OBJECTIVES

Cyber resiliency objectives are more specific statements of what a system must achieve in its operational environment and throughout its lifecycle to meet stakeholder needs for mission assurance and resilient security. The objectives[24] facilitate prioritization and assessment, making it straightforward to develop questions such as:

- 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?

Because stakeholders may find the statements of cyber resiliency objectives difficult to relate to their specific concerns, the objectives can be tailored or restated in terms or mission or business functions. In addition, representative methods for achieving each objective have been defined and help in understanding and defining metrics. The cyber resiliency objectives enable stakeholders to assert their different resiliency priorities based on mission or business functions. Table 3 provides a description of each cyber resiliency objective and representative examples of specific methods for achieving the objective.

[23] The conceptual 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].

[24] 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].

TABLE 3: CYBER RESILIENCY OBJECTIVES[25]

OBJECTIVE	DESCRIPTION	EXAMPLES OF METHODS TO ACHIEVE OBJECTIVES
Prevent or Avoid	Preclude the successful execution of an attack or the realization of adverse conditions.	• Apply basic cyber hygiene and risk-tailored controls. • Limit exposure to threat events. • Decrease the adversary's perceived benefits. • Modify configurations based on threat intelligence.
Prepare	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. Resources include not only cyber resources, but also personnel (with the proper training) and procedures. • Validate the realism of cyber courses of action. • Use validation methods that include testing or exercises.
Continue	Maximize the duration and viability of essential mission or business functions during adversity.	• Minimize degradation of service delivery. • Minimize interruptions in service delivery. • Ensure that ongoing functioning is correct.
Constrain	Limit damage[26] from adversity.	• Identify potential damage. • Isolate resources to limit future or further damage. • Move resources to limit future or further damage. • Change or remove resources and how they are used to limit future or further damage.
Reconstitute	Restore as much mission or business functionality as possible after adversity.	• Identify untrustworthy resources and damage.[27] • Restore functionality. • Heighten protections during reconstitution. • Determine the trustworthiness of restored or reconstructed resources.
Understand	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 cybersecurity and controls supporting cyber resiliency.
Transform	Modify mission or business functions and supporting processes to handle adversity and address environmental changes more effectively.	• Redefine mission / business process threads for agility. • Redefine mission / business functions to mitigate risks.
Re-Architect	Modify architectures to handle adversity and address environmental changes more effectively.	• Restructure systems or subsystems to reduce risks. • Modify systems or subsystems to reduce risks.
Shortcut to Table 4	Shortcut to Table H-1	Shortcut to Appendix F.2

[25] See Appendix H for specific relationships between objectives and goals.

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

[27] 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.

TAILORING CYBER RESILIENCY OBJECTIVES

Cyber resiliency objectives can be tailored to reflect the organization's missions and business functions or operational concept for the system-of-interest. Tailoring objectives can also help stakeholders determine which objectives apply and the priority to assign to each objective. The examples below illustrate the tailoring concept for cyber resiliency objectives:

- For an implantable medical device, the Continue objective can be tailored as follows: *Enable the patient or healthcare provider to engage fail-safe mechanisms*. The Constrain objective can be tailored as follows: *Ensure that the device can fail safely despite cyber-attacks, disruptions, or interference.*
- For a workflow system which is a constituent system of an organization's enterprise architecture, the Continue objective can be tailored by identifying critical business functions. The Constrain objective can be tailored as follows: *Limit damage from disruption and erroneous information.*

2.2.3 CYBER RESILIENCY TECHNIQUES AND APPROACHES

A cyber resiliency technique is a set or class of technologies and processes intended to achieve one or more goals or objectives by providing capabilities. Fourteen techniques are part of the cyber resiliency engineering framework as follows:

- Adaptive response;
- Analytic monitoring;
- Coordinated protection;
- Deception;
- Diversity;
- Dynamic positioning;
- Dynamic representation;
- Non-persistence;
- Privilege restriction;
- Realignment;
- Redundancy;
- Segmentation;
- Substantiated integrity; and
- Unpredictability.

The cyber resiliency techniques are defined in Appendix D. Each technique describes 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 cyber resiliency techniques can be applied to either adversarial or non-adversarial threats (including cyber-related and non-cyber-related threats). The two exceptions are Deception and Unpredictability. These techniques are only appropriate for addressing adversarial threats. The cyber resiliency techniques are also interdependent. For example, the Analytic Monitoring technique supports Dynamic Representation. The Unpredictability technique, however, is different than the other techniques in that it is always applied in conjunction with some other technique, for example, working in with Dynamic Positioning to establish unpredictable times for the repositioning of potential targets of interest.

TECHNIQUES AND APPROACHES APPLY SELECTIVELY

Applying a cyber resiliency technique typically will not require the use of all approaches which are representative of it, and not all techniques will be applied to a given system-of-interest. The following examples illustrate the application of cyber resiliency techniques and approaches.

- In a microgrid supplying and managing power for a campus, Deception can be applied sparingly. The Tainting approach will almost certainly not be applied. Whether Disinformation and Misdirection are applied will depend on the organization's risk management strategy. And while encryption of control messages may be viewed as an application of Obfuscation, its primary intention in this case would be to apply the Integrity Checks approach to Substantiated Integrity. Unpredictability will almost certainly not be applied to the campus microgrid system.
- Alternatively, an organization which interacts routinely with consumers via Internet-facing services can use all approaches to Deception, investing time and effort in maintaining a deception environment and analyzing interactions with adversaries from that environment. In addition, the organization can apply Unpredictability in conjunction with Deception and possibly with other techniques, such as Non-Persistence, Dynamic Positioning, and Privilege Restriction.

As noted above, cyber resiliency techniques provide ways to achieve one or more cyber resiliency objectives. The technique definitions are intentionally broad-based, to insulate the definitions from changing technologies and threats—thus limiting the need for frequent changes to the techniques. To support more detailed engineering analysis, multiple representative approaches to implementing each technique are identified. An approach is a subset of the technologies and processes included in a technique, defined by how the capabilities are implemented or how the intended outcomes are achieved. Appendix E defines the representative approaches and gives representative examples of technologies and practices. The set of approaches for a 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.[28]

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

2.2.4 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 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 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 will be selected, and those principles will be 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. 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., to be 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 F.

TAILOR DESIGN PRINCIPLES AND APPLY SELECTIVELY

Design principles are used to guide analysis and engineering decisions and to help stakeholders understand the rationale for those decisions. Therefore, design principles can be tailored in terms 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 supplying and managing 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, although 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 on how it provides offsite backup. Alternatively, the description of how the same design principle applies to a satellite constellation might refer to satellite maneuverability.

SELF-DRIVING CARS

Cyber resiliency is better understood when viewed through the prism of a use case. One such use case (i.e., the self-driving car) is presented below. As part of the use case discussion, the objectives and strategic design principles are restated to reflect the nature of the use case. The techniques and approaches are described relative to the vehicle functions. To facilitate readability, only the most applicable objectives, techniques, approaches, and design principles are listed below. Not all the listed techniques and approaches would be implemented; systems engineers would make the determination which of the techniques and approaches would be selected based on cost and operational considerations.

While the self-driving car (i.e., the system-of-interest) depends on other systems provided by multiple organizations (e.g., GPS, traffic management systems), the focus in this example is on cyber-enabled system elements within the vehicle. Consequences of greatest concern relate to the safety of passengers and of the environment (e.g., other vehicles, pedestrians). Other consequences of concern relate to potential failure to reach the intended destination (or to reach it by the required or predicted time); theft of the vehicle; and potential breaches of passenger privacy.

From a cyber resiliency **objectives** perspective, the highest-priority objectives are—

- **Prevent**: Prevent false geolocation, driving directions, and operating instructions from causing unsafe conditions.
- **Constrain**: Ensure that the car can fail safely despite cyber-attack, disruption, or interference.
- **Prepare**: Provide fail-safe mechanisms and supporting alerting mechanisms.
- **Continue**: Enable the driver to take control of the vehicle or to engage fail-safe mechanisms.

To achieve these objectives, the organization emphasizes the following **strategic design principles**:

- **Reduce attack surfaces**: Reduce the exposure of safety-critical system elements to non-safety-critical elements (e.g., the entertainment system).
- **Focus on common critical assets**: Protect the availability of the Controller Area Network (CAN) bus and the integrity of critical traffic to and from electronic control units (ECUs).

There are numerous cyber resiliency **techniques** and **approaches** that support the identified objectives. To facilitate readability, only a subset of the most applicable are listed below:

- Analytic Monitoring (Monitoring and Damage Assessment) – Use on-board sensors monitoring for indicators of anomalous and potentially adverse behavior which could affect vehicle safety, updated periodically based on threat data.
- Coordinated Protection (Calibrated Defense-in-Depth) – Employ increased levels of credential validation on commands to critical services especially regarding commands issued remotely.
- Coordinated Protection (Self-Challenge) – Use normal and security-enhanced diagnostics to validate security status.
- Non-Persistence (Non-Persistent Services) – Refresh from trusted sources, critical services when vehicle is not in motion (e.g., upon start-up).
- Privilege Restriction (Trust-Based Privilege Management) – Separate privilege assignment to critical (e.g., steering) and noncritical (entertainment) systems and services.
- Realignment (Restriction) – Remove unneeded connections between entertainment and vehicle-enabling systems.
- Segmentation (Predefined Segmentation) – Use cryptography to logically isolate networks supporting entertainment systems from those supporting vehicle control systems.
- Substantiated Integrity (Integrity Checks) – Use cryptographic checksums to validate authenticity of critical commands.

2.2.5 RELATIONSHIP AMONG CYBER RESILIENCY CONSTRUCTS

In addition to presenting cyber resiliency constructs in the form of goals, objectives, techniques, implementation approaches, and design principles (which systems engineers can use to express cyber resiliency concepts and the relationships among them), the relationship between cyber resiliency and risk management is also described. That relationship leads systems engineers to analyze cyber resiliency solutions in terms of their potential effects on risk and on the specific threat events or types of malicious cyber activities. As illustrated in Figure 1, 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 cyber resources—in particular, by risk framing.[29]

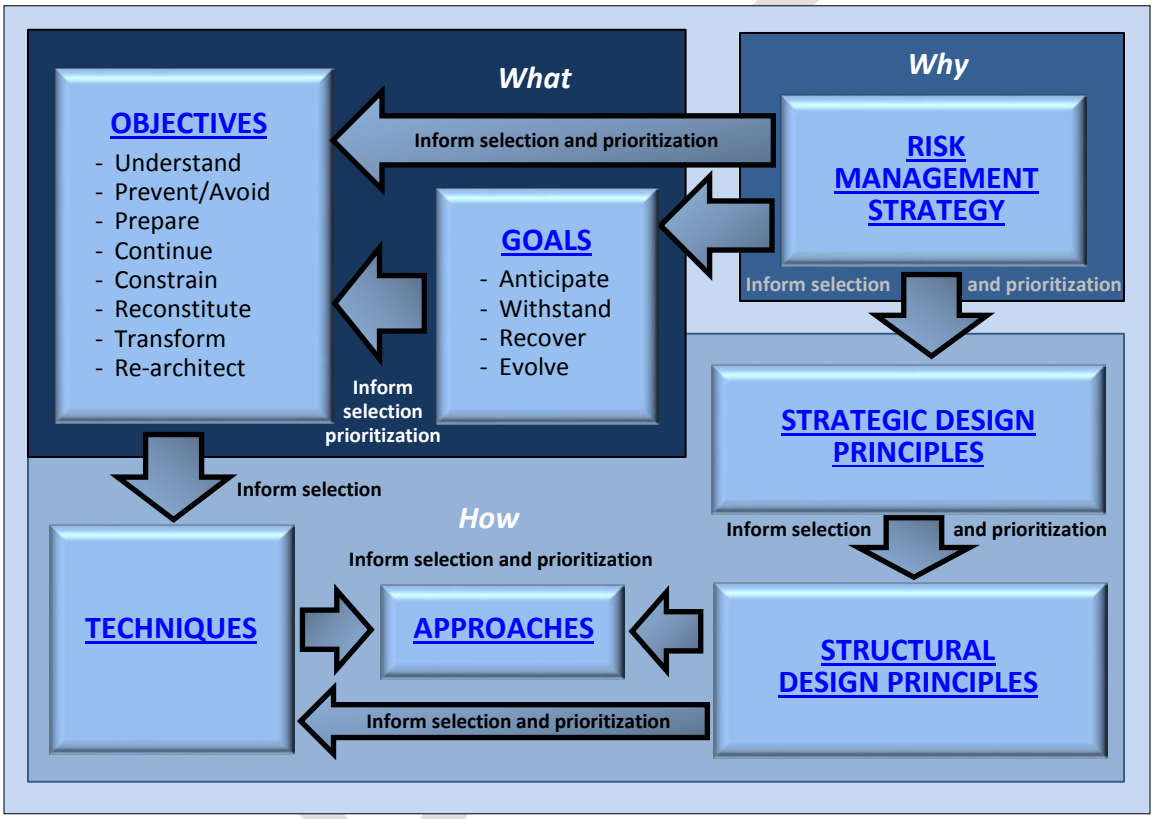

FIGURE 1: RELATIONSHIPS AMONG CYBER RESILIENCY CONSTRUCTS

The relative priority of the cyber resiliency goals and objectives, and the relevance of the cyber resiliency design principles, are determined by the risk management strategy of the organization. The relationships among the cyber resiliency constructs, represented by to specific mapping tables for the constructs, are summarized in Appendix H.

[29] 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 [NIST 800-39]. The risk management strategy addresses how the organization manages risks of depending on systems that include cyber resources and is part of a comprehensive enterprise-wide risk management strategy and reflects stakeholder concerns and priorities.

CYBER RESILIENCY ENGINEERING FRAMEWORK CONSTRUCTS

SUMMARY OF KEY RELATIONSHIPS

- The organization or project *risk management strategy* guides and informs the selection and prioritization of cyber resiliency goals and objectives and strategic design principles.
  Achieving cyber resiliency objectives supports achieving cyber resiliency goals.
- Cyber resiliency *goals* and *objectives* inform the selection and prioritization of cyber resiliency techniques.
  Applying cyber resiliency techniques supports achieving cyber resiliency goals and objectives.
- Cyber resiliency *techniques* inform the selection and prioritization of cyber resiliency approaches.
  Cyber resiliency approaches describe ways to implement cyber resiliency techniques.
- Cyber resiliency *strategic design principles* inform the selection and prioritization of structural design principles which influences the selection of techniques and approaches.
  Applying cyber resiliency design principles supports the realization of cyber resiliency goals and objectives.

2.3 CONCEPT OF USE

The following sections describe general considerations for applying cyber resiliency concepts and framework constructs to system life cycle processes. Chapter Three provides additional details on how these considerations apply to the system life cycle processes defined in [NIST 800-160, Vol. 1]. Considerations also include addressing the similarities and differences in security and cyber resiliency terminology and how the application of cyber resiliency goals, objectives, techniques, approaches, and design principles can impact systems at key stages in the life cycle.

2.3.1 LIFE CYCLE CONCEPT

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. These tailoring actions are used to elicit stakeholder priorities for the cyber resiliency goals and objectives. Aspects of the organization's risk management strategy which frame risk, are used to determine which strategic design principles are most relevant. These principles, and the 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, aspects of the organization's risk management strategy which constrain risk response (e.g., commitment to specific technologies, requirements for interoperability with, or dependence on, other systems) are used to help determine which techniques and approaches can or cannot be used in cyber resiliency solutions.

During the *Development* stage, relevant structural cyber resiliency design principles (i.e., those 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 they enable the

prioritized cyber resiliency objectives to be achieved. Cyber resiliency techniques and approaches indicated by the relevant structural design principles are analyzed with respect to whether and where they can be used in the selected system architecture, subject to 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 against potential threat events or scenarios and the measures of effectiveness for cyber resiliency objectives. Analysis of compatibility with other aspects of trustworthiness considers potential synergies or conflicts 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 cyber resiliency contributing or 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 which includes 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. During this 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 to associated spare parts or components. The verification strategy for the cyber resiliency requirements as applied to such system elements includes adversarial testing or demonstration in a stressed environment. In addition, cyber resiliency concerns for enabling systems for production, integration, and validation, and for supply chain management, are 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 threat environment (e.g., new threat actors, newly discovered vulnerabilities in commonly used technologies), the operational environment (e.g., new mission or business processes, increased user population, deployment in new locations, addition or removal of other systems with which the system-of-interest interacts), 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., by defining new courses of action, by changing mission or business processes and procedures, by 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. Upgrade or modification of system capabilities can include significant architectural changes to address accumulated changes to the operational, threat, and technical environments. 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, for example, 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. And 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.
Development	• Use techniques and approaches to define alternative solutions. • Apply design principles to refine and analyze 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).

2.3.2 CYBER RESILIENCY AND SYSTEMS SECURITY ENGINEERING TERMINOLOGY

Several phrases are integral to the statement and elaboration of the activities and tasks in systems security engineering processes. These include, for example: security aspects; security objectives; security models; concept of security function; security criteria; security requirements; security-driven constraints; and security-relevant as applied to a variety of terms. To overcome any potential confusion in this publication, the tailoring of statements and elaborations to address

cyber resiliency will frequently replace the term *security* with *security and cyber resiliency*. The interpretation of the key phrases will change accordingly, as indicated in general terms below.

2.3.2.1 SECURITY AND CYBER RESILIENCY ASPECTS

The interpretation of the term *security aspect* is context-dependent. In the *Agreement Processes* described in [NIST 800-160, Vol. 1], the security aspects of an acquisition involve protecting information and enabling systems, and generally do not involve cyber resiliency. Therefore, the meaning of security aspect is unchanged for those processes. However, the scope of project management processes may include enabling systems. Depending on how the organization's risk management strategy treats risks to enabling systems, and how it treats supply chain risks, *Organizational Project-Enabling Processes* may need to consider security and cyber resiliency aspects rather than simply security aspects.

In the context of *Technical Processes*, security aspects may not include cyber resiliency aspects. For purposes of illustration, two examples are presented; the cyber resiliency aspects of other technical processes are described in the Cyber Resiliency Engineering Purpose or Discussion sections of those processes.

For a *problem* (or opportunity) in the *Business or Mission Analysis* process in [NIST 800-160, Vol. 1], the cyber resiliency aspects include the relative priorities of cyber resiliency goals to different stakeholders; how cyber resiliency objectives are tailored and prioritized by different stakeholders; and what constraints will limit the applicability of cyber resiliency techniques, approaches, and design principles, and thereby will limit how alternative solutions are defined and selected. Similarly, the cyber resiliency aspects of an *opportunity* (e.g., insert a new technology, replace a legacy system element, change a mission or business process to use system elements in a new way) include changes in which cyber resiliency approaches, techniques, or design principles are applied, or in how they could be applied, and consequently which cyber resiliency objectives can be achieved and to what extent. The cyber resiliency aspects of a *solution* include which cyber resiliency approaches, techniques, and design principles are applied; how they could be applied (e.g., at what architectural locations, in conjunction with which security capabilities or design principles); and which cyber resiliency objectives are or can be achieved and to what extent.

The security aspects of a verification or a validation strategy as described in the *Verification* and *Validation* processes in [NIST 800-160, Vol. 1] can include some cyber resiliency aspects. Such strategies can include or can be organized around a set of threat scenarios. Cyber resiliency considerations in a verification or a validation strategy include verification or validation of the system's ability to achieve its mission or business objectives in the face of attacks motivated by anticipated adversary goals (as defined in the organization's risk management strategy); and under the assumption that different system elements have been compromised (i.e., have become untrustworthy). The cyber resiliency aspects of the strategy, therefore, need to identify other systems which will be represented in verification or validation procedures, how the systems will be represented (e.g., by using enabling systems for emulation of other systems, or for fault injection), and what assumptions about their behavior or trustworthiness properties will be represented. In addition, the cyber resiliency aspects of the strategy need to consider how to represent cascading failures, propagation of malware or incorrect data, ripple effects of threat events, and loss due to unknown reasons.[30]

[30] This may be represented by some communities as a *threat tree*.

2.3.2.2 SECURITY AND CYBER RESILIENCY CRITERIA

In systems engineering, *criteria* are principles or standards of judgment regarding whether and how well a supplier can conform to laws, directives, regulations, policies, or business processes; whether and how well a supplier can deliver the requested product or service in satisfaction of the stated requirements and in conformance with required business practices; the ability of a specific mechanism, system element, or system to meet its 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; how a delivered product or service is handled, distributed, and accepted; how to perform verification and validation; or how to store system elements in disposal. Criteria related to a system's ability to meet requirements may be expressed in quantitative terms (i.e., metrics and threshold values), in qualitative terms (including threshold boundaries), or in terms of identified forms of evidence.

Security criteria are security-relevant criteria, and can be complemented by cyber resiliency criteria in certain instances. *Cyber resiliency criteria* are criteria regarding whether and how well an architecture or design of a system or system element conforms with cyber resiliency design principles; whether and to what extent an architecture, design, or implementation incorporates selected cyber resiliency techniques or approaches; whether and to what extent an architecture, design, or implementation can be expected to achieve cyber resiliency objectives (as selected or tailored); how and the extent to which an architecture, design, or implementation manages risk or affects the activities of a cyber adversary; or how and the extent to which an architecture, design, or implementation enables mission or business objectives to be achieved in the face of adversity, particularly adversity involving the APT. Like security criteria, cyber resiliency criteria can be expressed in quantitative or qualitative terms. Cyber resiliency criteria are often defined or expressed as measures of performance (MOPs), measures of effectiveness (MOEs), or other metrics evaluated under adversarial conditions.

2.3.2.3 SECURITY AND CYBER RESILIENCY REQUIREMENTS AND CHARACTERISTICS

The definition of *security requirement* in [NIST 800-160 Vol. 1] is quite broad: a "requirement that specifies the functional, assurance, and strength characteristics for a mechanism, system, or system element." In this publication, therefore, security requirements include cyber resiliency requirements, just as controls in [NIST 800-53] include controls related to security, privacy, and cyber resiliency. However, there are some security requirements that are specifically motivated by cyber resiliency concerns. For brevity, the term *cyber resiliency requirement* is used to mean a security requirement which is traceable to a cyber resiliency objective or design principle, or which requires the use of a cyber resiliency technique or approach. Cyber resiliency requirements assume the compromise of system elements by an adversary, and are traceable to mission or business needs to achieve the resilience goals of anticipate, withstand, recover, and adapt.

The term *security characteristics* includes the security functions the system performs; the security-relevant capabilities the system provides; the level of assurance in the correctness of those functions and in the consistent enforcement of security policies, even under conditions of stress; and the concept of security function embodied in the system architecture and design. For brevity, the term *cyber resiliency characteristics* means the security characteristics related to the need to achieve the resiliency goals of anticipate, withstand, recover, and adapt, in the face of the compromise of system elements (or the system) by an adversary and adversary activities.

2.3.2.4 CYBER RESILIENCY AND THE CONCEPT OF SECURITY FUNCTION, VIEWS, AND MODELS

Several terms are central to understanding and executing the *Architecture Definition*, *System Analysis*, *Implementation*, *Integration*, and *Verification* processes in [NIST 800-160, Vol.1], including the concept of secure function, security viewpoints, security views, and security models. The *concept of secure function* is a strategy for system security and includes the protection strategies, methods, and techniques used to apply security design principles and concepts to the system architecture. From a cyber resiliency perspective, the concept of secure function defines a strategy for achieving cyber resiliency objectives, applying cyber resiliency design principles, and using cyber resiliency techniques and approaches, consistent with and integrated with the strategy for system security.

A *security viewpoint* (a work product from the systems engineering process) expresses or is driven by the concept of secure function. A security viewpoint identifies the security principles, model types, concepts, correspondence rules, methods, and analysis techniques that are provided by the *security view*.[31] A set of one or more security viewpoints specifies a security view of an architecture (also a work product of the systems engineering process). The security view and viewpoints address concerns for controlling the loss of assets and the associated consequences of asset loss. In principle, cyber resiliency views and viewpoints can be integrated into security views and viewpoints. However, development of a cyber resiliency view as a separate work product, or as a separate section of a security view work product, enables systems security engineering tasks to focus on whether and how an architecture (and subsequently, a design, an implementation, and an integrated system) achieves the cyber resiliency objectives and addresses stakeholder concerns related to threat activities and compromised resources. Similarly, a cyber resiliency viewpoint, as a separate work product or as a separate section of a security viewpoint work product, can identify cyber resiliency design principles, concepts, model types, and analysis techniques, and can relate these to the corresponding topics in security viewpoints.

A *security model* is a representation of an architecture, design, or system which identifies entities and relationships (e.g., subjects, objects, and a reference monitor; enclaves, boundaries, and information flows; information sources, destinations, and communications paths) in such a way that conformance with security requirements and enforcement of security policies can easily be analyzed. A security model uses or relies on an architecture framework, and can be a physical, logical, or information model. A *cyber resiliency model* is either behavioral or structural. A *behavioral* cyber resiliency model represents the behavior of a system (at a given architectural layer or range of layers), to facilitate analysis of the cyber effects of adverse events on systems and on system behavior; system behavior with respect to business or mission performance requirements, including security performance under a variety of adverse conditions; and the effects of cyber resiliency solutions or cyber courses of action. Many cyber resiliency models explicitly represent adversarial behavior. A *structural* cyber resiliency model identifies where and how, within a system architecture, cyber resiliency techniques and approaches are implemented, or cyber resiliency design principles are applied. Both types of cyber resiliency models support cyber resiliency analysis techniques (See Section 2.5). Both cyber resiliency models and cyber resiliency analysis techniques explicitly assume that some resources are untrustworthy. While a cyber resiliency model can be an instance of or an integral part of a security model, more often a mapping between the two types of models is needed. Cyber resiliency models do not represent policy requirements, but typically represent adverse events (e.g., adversary behavior, environmental disruption) in a temporal rather than state-transition way.

[31] [NIST 800-160, Vol.1] provides additional information on security views, security viewpoints, and security models.

2.4 ENGINEERING CONSIDERATIONS

As noted earlier, fourteen cyber resiliency techniques and nearly fifty cyber resiliency approaches have been identified. There is no single best resiliency technique or approach. Nor is there a minimum set of resiliency techniques or approaches to be applied to a system. The choice of the optimum set of resiliency techniques and implementation 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 neither feasible nor possible to employ all techniques and approaches. The sections that follow describe factors to consider in selecting the optimum resiliency techniques and associated resiliency approaches.

2.4.1 ACHIEVEMENT OF GOALS AND OBJECTIVES

Cyber resiliency techniques and associated implementation approaches are employed to achieve mission or business objectives in an operational context. The relative priorities of cyber resiliency goals and objectives are determined by the mission or business objectives. As noted previously, different cyber resiliency objectives support different cyber resiliency goals, and different cyber resiliency techniques and approaches support different cyber resiliency objectives. Techniques or approaches which support the higher-priority objectives are the top candidates for selection, while techniques which support objectives which have low or no priority are unlikely to be useful.

2.4.2 RISK MANAGEMENT STRATEGY

An organization's risk management strategy (i.e., its strategy for managing risks of depending on systems which include cyber resources) includes its risk framing. For cyber resiliency, the risk frame assumes the APT, 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 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 also 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 tailored to a given program, mission, business function, or system, such an order of precedence can guide the selection and application of structural design principles at different locations in an architecture.

2.4.3 TAILORING TO THE TYPE OF SYSTEM

The set of cyber resiliency techniques and approaches which are most relevant to and useful in a system depends on the type of system.

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

  These are typically general-purpose systems, often with significant processing, storage, and bandwidth capabilities, 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 cyber resiliency techniques and associated approaches may potentially be viable, although their selection would be filtered based on the other considerations noted in this section.

- **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 benefit than others. For example, Dynamic Representation, implemented via Mission Dependency and Status Visualization, can be applied to enable prediction of 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 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 which were not designed to work together and which were developed with different missions and risk frames, the Realignment technique could also be beneficial. The Purposing, Offloading, and Restriction approaches could also be very useful in ensuring that the core system elements are appropriately aligned to the overall system-of-system mission. Note that the above techniques and approaches are highlighted for illustrative purposes. There are other techniques and approaches that could be useful for a system-of-systems environment, and the specific aspects of the system-of-systems in question will impact the selection as well.

- **Critical Infrastructure Systems**

  These systems are often specialized, high-confidence, dedicated, purpose-built systems that have highly deterministic properties. As such, they often have limitations regarding storage and processing capabilities; strict timing constraints; and severe, if not catastrophic, consequences of failure. Therefore, the availability and integrity of the functionality of the systems is very important as the corruption or lack of availability of some of the key system elements could result in very significant harm to a large number of the population. For these reasons, techniques adapted from cyber resiliency, 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 maximize the chance of continuation of the critical or essential mission or business operations. Segmentation can isolate highly critical system elements that protect it 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. The above techniques and approaches are highlighted for illustrative purposes; other techniques and approaches could be useful in critical infrastructure protection, and the specific aspects of the systems in question will impact the selection as well.

- **Cyber-Physical Systems**

  As with critical infrastructure systems, cyber-physical systems often have significant limitations regarding storage capacity, processing capabilities, and bandwidth. In addition, many of these systems often have a high degree of autonomy with very limited human interaction. Some cyber-physical systems often operate in stand-off mode (i.e., no network connection). Non-Persistent Services support the periodic refreshing of software and firmware from a trusted source (e.g., an off-line 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 enable embedded systems to detect corrupted software components. These techniques and

approaches are offered for illustrative purposes; there are other techniques and approaches that could be useful in embedded systems.

2.4.4 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, 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 Dynamic Representation more difficult; a design which incorporates Diversity requires monitoring tools which 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 design principles and the risk management strategy, synergies and conflicts between various techniques should be taken into consideration. The text below offers some illustrative examples of the interplay.

For example, Dynamic Positioning and Non-Persistence enable operational agility by making it more difficult for an adversary to target critical resources; 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. But at the same time, those techniques (and the associated implementation approaches) also make it more difficult for an organization to maintain situational awareness of its security posture, in effect complicating the use of Dynamic Representation and aspects of Analytic Monitoring, and undermining the application of the Maintain situational awareness structural design principle. Similarly, Redundancy and Diversity together are very effective in resisting adversary attacks; enhance the organization's ability to achieve the Continue and Reconstitute objectives; and apply the Plan and manage diversity and Maintain redundancy structural design principles. But the implementation of both Redundancy and Diversity will increase the organization's attack surface. In general, while Redundancy, Diversity, 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 Appendix D.

2.4.5 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., cybersecurity, COOP) but are used or executed in a different manner to support cyber resiliency. Others are drawn from disciplines that deal with non-adversarial threats (e.g., safety). Still others are cyber adaptations of non-cyber concepts drawn from disciplines that deal with adversarial threats (e.g., medicine, military, sports).

The nature of the legacy investments made by an organization in these other disciplines can influence which cyber resiliency techniques and approaches are most appropriate to pursue. If an organization has invested heavily in certain technology designed to support COOP, but with some modifications can support cyber resiliency, that is a reasonable consideration in the selection of cyber resiliency techniques and approaches—that is, building on the existing investments.

2.4.5.1 INVESTMENTS FROM CYBERSECURITY, COOP, AND RESILIENCE ENGINEERING

Redundancy-supporting approaches such as backup, surplus capacity, and replication are well established in COOP. In cyber resiliency, there is a recognition that these approaches are by themselves 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 equally vulnerable to malware that has compromised the primary server. But 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 or authentication challenges (Calibrated Defense-in-Depth approach to Coordinated Protection) or some form of Synthetic Diversity to compensate for known attack vectors.

Both Dynamic Representation and Analytic Monitoring capabilities are often provided by cybersecurity and performance management functions such as cyber situational awareness, anomaly detection, and performance monitoring. But the normal, off-the-shelf implementations of these functions are generally insufficient to detect threats from advanced adversaries whose actions are very stealthy. Enhancing existing investments in detection and monitoring by trying to fuse together sensor and monitor readings from disparate sources is a way to take these existing investments and make them an effective cyber resiliency tool. Still another way to make existing technology more cyber resilient-focused is by complementing the existing monitoring services with information from threat intelligence sources enabling these tools to be better tuned to look for known observables (e.g., 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 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. But ensuring that those protections work in a coordinated fashion is one of the distinguishing aspects of cyber resiliency.

2.4.5.2 INVESTMENTS FROM NON-ADVERSARIAL DISCIPLINES

Some cyber resiliency techniques and approaches come from disciplines such as safety. Diversity and certain implementations of Substantiated Integrity, such as Byzantine quorum systems[32] or checksums on critical software, can be traced back to the safety discipline.[33] Therefore, systems that have been designed with safety in mind may already have implemented some of these

[32] The National Aeronautics and Space Administration (NASA) space shuttle applied this concept in multiple computers which would vote on certain maneuvers.

[33] 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.

capabilities. The difference is that 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. But 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. Capabilities such as Non-Persistence are very common in cloud and virtualization architectures. Again, this capability was not designed or employed to 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., to periodically with the goal of flushing out malware) than it is to deploy non-persistence in a system that never had the capability in the first place.

2.4.5.3 INVESTMENTS FROM ADVERSARIAL DISCIPLINES

Several of the cyber resiliency techniques and approaches are cyber adaptions of non-cyber measures used in adversarial/conflict disciplines (e.g., military, sports). These include Deception, Unpredictability, Dynamic Positioning, and the Adaptive Management approach to implementing Adaptive Response. None of those cyber resiliency techniques or approaches would be employed in non-adversarial disciplines; there 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 very well established. Because these adversarial-derived techniques and approaches are not typically found in disciplines such as safety, resilience engineering, COOP, information security, or cybersecurity, it is much more challenging to provide them by enhancing existing constructs. Therefore, they may be more challenging to integrate into an existing system.

2.4.6 ARCHITECTURAL LOCATIONS

Different techniques or approaches lend themselves to implementation at different architectural layers. For example, relatively few approaches can be implemented at the physical layer. These include Dynamic Reconfiguration, Architectural Diversity, Design Diversity, Asset Mobility, Replication, Predefined Segmentation, and Integrity Checks. Depending on the scope of the acquisition or the architecture into which the system-of-interest must fit, some approaches may be infeasible.

2.4.7 EFFECTS ON ADVERSARIES, THREAT, AND RISK

The linkage between cyber resiliency techniques or approaches and effects is in terms of 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 likelihood of impact or reduce level of impact) than others. The security mechanisms or processes used to implement a 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 holistic suite of intrusion detection systems, both will

achieve the effect detect. But 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. 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 the flexibility of evolving and tailoring the effects to adversary's changing actions. In some ways, this is analogous to team sports where the one team will change its game plan in response to player injuries and the changing game plan of the other team. A team with players that can play multiple positions gives it flexibility to respond to changes by the opposition and to potentially replace injured players with others that can play the position of the injured player.

Different cyber resiliency techniques and approaches can have different effects on threat events and on 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. Appendix I describes the potential effects cyber resiliency can have on adversary activities, threats, and risk.

2.4.8 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 on its strategy for managing technical risks. Many highly mature and widely adopted technologies and processes that were developed to meet general needs for 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, and thereby reducing risks due to the APT, should be balanced against risks associated with perturbing such systems.

2.5 ANALYTIC PRACTICES

Cyber resiliency engineering leverages and extends a variety of existing analytic practices from the domains of security, systems engineering, resilience engineering, cybersecurity, and mission assurance. Examples of analytic practices include:

- **Security:** Operations security (OPSEC) analysis;
- **Systems Engineering:** Modeling and simulation (M&S), model-based systems engineering (MBSE), and Functional Dependency Network Analysis (FDNA);
- **Resilience Engineering:** Mission Impact Analysis (MIA), Business Impact Analysis (BIA), fault tree analysis, and Failure Modes, Effects, and Criticality Analysis (FMECA);
- **Cybersecurity:** Coverage analysis with respect to a taxonomy of attack events or TTPs, attack tree or attack graph analysis, attack surface analysis, and Red Team analysis; and
- **Mission Assurance:** Crown Jewels Analysis (CJA), mission thread analysis, Cyber Mission Impact Analysis (CMIA), and supply chain risk management (SCRM).

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

CHAPTER THREE

CYBER RESILIENCY IN SYSTEM LIFE CYCLE PROCESSES

APPLYING CYBER RESILIENCY CONCEPTS AND CONSTRUCTS IN SYSTEMS LIFE CYCLE PROCESSES

This chapter describes the cyber resiliency considerations and contributions to system life cycle processes to produce the cyber resiliency outcomes that are necessary to achieve trustworthy securely resilient systems. The considerations and contributions are provided as selective and specific modifications to the systems security engineering activities and tasks in [NIST 800-160, Vol. 1] and are aligned with and developed as cyber resiliency extensions to the system life cycle processes in [ISO/IEC/IEEE 15288]. Figure 2 lists the system life cycle processes and illustrates their application across all stages of the system life cycle. The initial scope of this publication is limited to the Technical Processes described in ISO/IEC/IEEE 15288.[34]

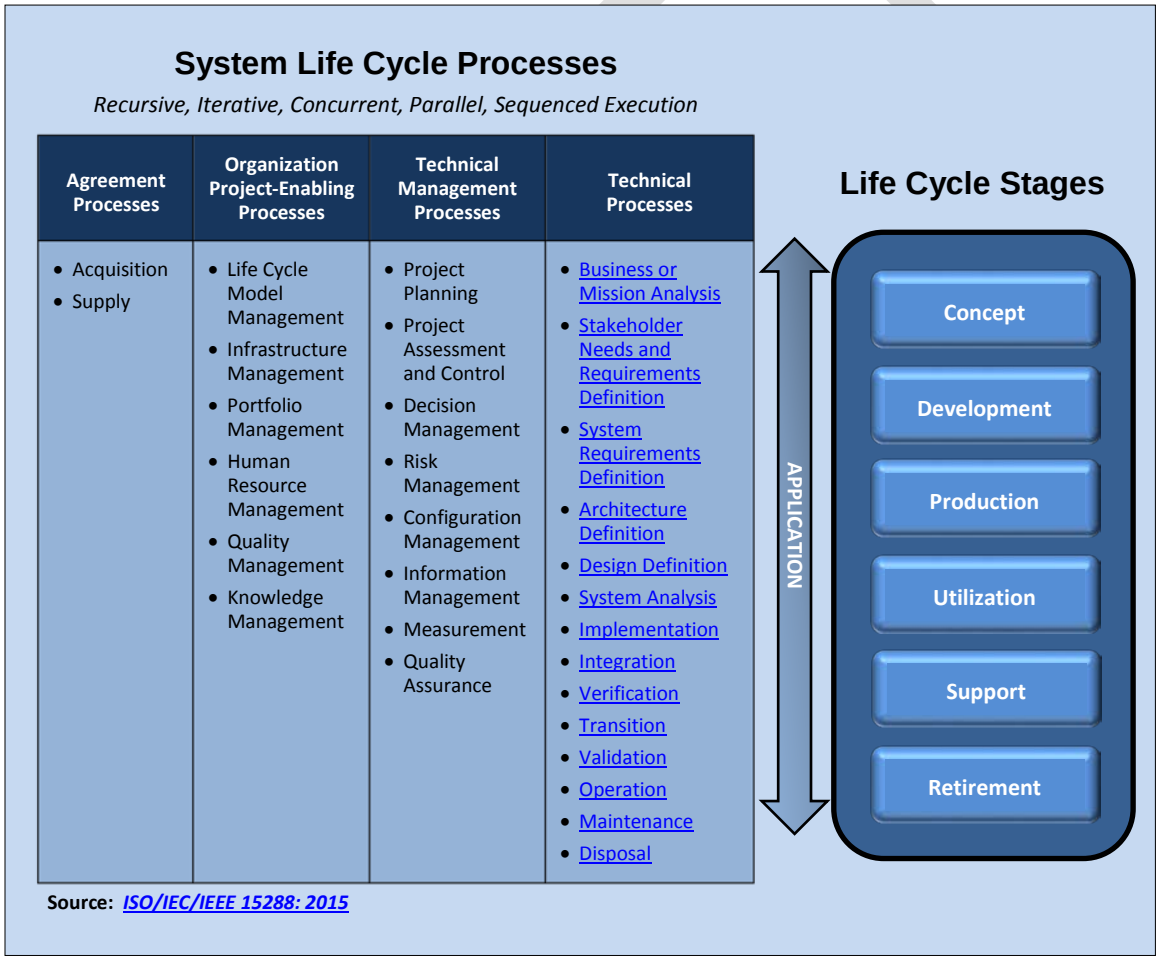

FIGURE 2: SYSTEM LIFE CYCLE PROCESSES AND LIFE CYCLE STAGES

[34] Subsequent iterations of this publication will address the nontechnical processes that compose the Agreement Processes, Project Processes, and Project-Enabling Processes.

Cyber resiliency is addressed in conjunction with the closely related concerns of system resilience and security. The focus of analysis for cyber resiliency is on meeting system requirements and addressing stakeholder concerns in the face of attacks on systems by the APT. Cyber resiliency focuses on capabilities used to ensure accomplishment of mission or business functions, for example, 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 missions or business functions, and thus complement the more established security objectives of confidentiality, integrity, and availability that apply to information and to information systems. 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. Due to this complementarity, cyber resiliency can be incorporated into existing security activities and tasks described in the systems life cycle processes in [NIST 800-160, Vol. 1]. No new processes are needed, nor are any new activities or tasks needed for the existing processes. Resiliency offers new considerations for these existing processes, activities, and tasks. However, given that the language in the processes is not cyber resiliency-specific, it may not always be obvious how and where cyber resiliency might be injected into the engineering processes.

The following sections provide specific cyber resiliency considerations for the system life cycle processes, activities, and tasks in [NIST 800-160, Vol. 1]. In many cases, no changes are needed. In other cases, a simple replacement of the term "security" with "security and cyber resiliency" suffices, with the understanding that material in Chapter Two and the supporting appendices will be consulted if additional discussion on a specific life cycle process is needed. Representative examples of such discussion are presented for selected tasks. Those examples illustrate how, although consideration of cyber resiliency is consistent with existing tasks, the underlying assumptions and constructs of cyber resiliency require explicit discussion for some tasks.

As applicable, the *discussion* sections will note where specific cyber resiliency constructs are explicitly cited, where the emphasis of cyber resiliency is different. The discussion is intended to be illustrative and thorough, but not exhaustive. Other activities and tasks for which discussion is not presented in this appendix may still be relevant to cyber resiliency. Considerations for cyber resiliency are addressed for the fourteen *Technical* processes in [ISO/IEC/IEEE 15288]. The remaining *Agreement*, *Project-Enabling*, and *Technical Management* processes will be addressed in future updates to this publication.

3.1 BUSINESS OR MISSION ANALYSIS

Cyber Resiliency Engineering Purpose

When considering cyber resiliency as part of the *Business or Mission Analysis* process, systems security engineering analyzes business or mission problems or opportunities from the perspective of cyber resiliency goals, objectives, and constraints on the solution space. The problem space is assumed to include activities and attacks by APT actors, which can have asset loss consequences, and cause damage to other systems or incur risks at a larger scope or scale than for the system-of-interest. This process identifies and prioritizes cyber resiliency objectives, which can be tailored specifically for the organization, stakeholders, or the system-of-interest. In addition, this process identifies constraints or limitations on the solution space. Constraints on the selection of cyber resiliency techniques and approaches may be related to the type of system, may be architectural constraints such as interoperability with a specific product suite or conformance to standards, or may result from the organization's risk management strategy (e.g., maturity of solutions, policy regarding deception). Constraints on the selection of cyber resiliency design principles may be related to the organization's risk management strategy, the selection of security design principles with which cyber resiliency design principles must be aligned, or design principles from other specialty engineering disciplines.

Cyber Resiliency Engineering Outcomes

- Cyber resiliency goals are prioritized.
- Cyber resiliency objectives are tailored and prioritized.
- Assumptions regarding the capability of adversaries are identified.
- Constraints or limitations on the cyber resiliency techniques, approaches, and design principles are identified.
- Measures of success for cyber resiliency objectives are identified.

Cyber Resiliency Considerations

BA-1.2 Review organizational problems and opportunities with respect to desired security **and cyber resiliency** objectives.

Discussion: Security and cyber resiliency objectives must be achieved despite adversity which includes a variety of APT activities and attacks. Cyber resiliency goals and objectives are tailored in organizationally meaningful terms, and prioritized to reflect stakeholder concerns.

BA-2.1 Analyze the problems or opportunities in the context of the security **and cyber resiliency** objectives and measures of success to be achieved.

Discussion: Problems include potential consequences to stakeholders, mission or business functions, and other systems, as well as to the system-of-interest and its assets, due to adversary activities and attacks. The (tailored and prioritized) cyber resiliency objectives are used to identify measures of success.

BA-3.1 Define the security **and cyber resiliency** aspects of the preliminary operational concepts and other concepts in life cycle stages.

Discussion: Cyber resiliency considerations inform the integration of cyber courses of action into security operational concepts, particularly for operational scenarios involving APT activities and attacks, in which the system must be securely resilient.

Table 5 lists the cyber resiliency considerations for the *Business or Mission Analysis* process.

TABLE 5: CYBER RESILIENCY CONSIDERATIONS FOR MISSION OR BUSINESS ANALYSIS

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
BA-1	PREPARE FOR THE SECURITY ASPECTS OF BUSINESS OR MISSION ANALYSIS	Change "security aspects" to "security and cyber resiliency aspects."
BA-1.1	Identify stakeholders who will contribute to the identification and assessment of any mission, business, or operational problems or opportunities.	No change.
BA-1.2	Review organizational problems and opportunities with respect to desired security objectives.	Change "security objectives" to "security and cyber resiliency objectives." See Discussion.
BA-1.3	Define the security aspects of the business or mission analysis strategy.	Change "security aspects" to "security and cyber resiliency aspects."
BA-1.4	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of the business or mission analysis process.	No change.
BA-2	DEFINE THE SECURITY ASPECTS OF THE PROBLEM OR OPPORTUNITY SPACE	Change "security aspects" to "security and cyber resiliency aspects."
BA-2.1	Analyze the problems or opportunities in the context of the security objectives and measures of success to be achieved.	Change "security objectives" to "security and cyber resiliency objectives." See Discussion.
BA-2.2	Define the security aspects and considerations of the mission, business, or operational problem or opportunity.	Change "security aspects" to "security and cyber resiliency aspects."
BA-3	CHARACTERIZE THE SECURITY ASPECTS OF THE SOLUTION SPACE	Change "security aspects" to "security and cyber resiliency aspects."
BA-3.1	Define the security aspects of the preliminary operational concepts and other concepts in life cycle stages.	Change "security aspects" to "security and cyber resiliency aspects." See Discussion.
BA-3.2	Identify alternative solution classes that can achieve the security objectives within limitations, constraints, and other considerations.	Change "security objectives" to "security and cyber resiliency objectives."
BA-4	EVALUATE AND SELECT SOLUTION CLASSES	No change.
BA-4.1	Assess each alternative solution class taking into account the security objectives, limitations, constraints, and other relevant security considerations.	Change "security objectives" to "security and cyber resiliency objectives."
BA-4.2	Select the preferred alternative solution class (or classes) based on the identified security objectives, trade space factors, and other criteria defined by the organization.	Change "security objectives" to "security and cyber resiliency objectives."
BA-5	MANAGE THE SECURITY ASPECTS OF BUSINESS OR MISSION ANALYSIS	No change.
BA-5.1	Maintain traceability of the security aspects of business or mission analysis.	No change.
BA-5.2	Provide security-relevant information items required for business or mission analysis to baselines.	No change.

3.2 STAKEHOLDER NEEDS AND REQUIREMENTS DEFINITION

Cyber Resiliency Engineering Purpose

When considering cyber resiliency as part of the *Stakeholder Needs and Requirements Definition* process, systems security engineering elicits stakeholder needs for cyber resiliency and translates those needs into cyber resiliency requirements. Stakeholder needs can be expressed in terms of methods for achieving cyber resiliency objectives by tailoring and prioritizing the objectives. The relevance of different methods for achieving a particular cyber resiliency objective depends on the constraints on the solution space identified previously, and in particular on the preliminary operational concept. Stakeholder needs take asset susceptibility with regards to the APT into consideration. Because of the persistence, capability, and stealth of the APT, this threat should be carefully considered in this process. Finally, relevant strategic cyber resiliency design principles are identified, consistent with the risk management strategy of the organization.

Cyber Resiliency Engineering Outcomes

- Relevant methods for achieving cyber resiliency objectives are identified and tailored in terms meaningful to the stakeholders and the system-of-interest.
- The methods for achieving cyber resiliency objectives are translated into stakeholder requirements.
- Asset susceptibility to APT-like adversaries is determined.
- The relevant strategic cyber resiliency design principles are identified.

Cyber Resiliency Considerations

SN-2.1 Define the security context of use across all preliminary life cycle concepts.

Discussion: From a cyber resiliency perspective, the security context of use includes consideration of users, other stakeholders, and individuals, organizations, other systems in the environment of operations and enabling systems in the supply chain (collectively, environmental entities) in multiple ways: as a threat source (either intentional or unintentional); as attack surfaces extending the attack surface of the system-of-interest; and as potential elements of the cyber resiliency solution space. For example, including a service that facilitates an organization's ability to refresh the system or system elements (perhaps employing a virtualization capability) as part of the solution space would facilitate applying the Maximize transience design principle as well as the Change or disrupt attack surface design principle). Therefore, the context-of-use description identifies the relationships, including legal, contractual, or technical, which apply to environmental entities.

SN-2.3 Prioritize assets based on the adverse consequence of asset loss.

Discussion: Stakeholder concerns for asset loss generally include loss of sensitive information, availability of services, information quality, and direct consequences of damage to the mission or business functions which depend on those assets. However, from a cyber resiliency perspective, indirect consequences of asset loss are also considered. For example, corrupted information or loss of service reliability can undermine user confidence, lead users to change their usage patterns, and ultimately damage the reputation of the organization. In addition, assets should be identified and prioritized from an adversary's perspective; an asset which initially appears to have low priority to stakeholders can be a high-value target to an adversary. Finally, since damage to the system can have cascading adverse effects on other systems and organizations, assets should be identified and prioritized at multiple levels or scopes.

SN-2.7 Define the stakeholder protection needs and rationale.

Discussion: From the standpoint of cyber resiliency, stakeholder protection needs can be expressed as methods or capabilities needed to achieve cyber resiliency objectives. These can subsequently be translated into stakeholder cyber resiliency requirements, once the rationale for prioritizing them and making trade-offs among them are captured. For example, some stakeholders may be most concerned with minimizing the propagation of APT-related malware to maximize mission or business accomplishments. In contrast, other stakeholders may be more interested in gaining insight into the nature of the adversary malware to be better positioned to develop mitigations to that malware which can be applied beyond the confines of the system. Stakeholder protection needs can also be defined or described in terms of a risk management strategy, and then expressed in terms of strategic cyber resiliency design principles.

SN-5.4 Resolve stakeholder security requirements issues.

Discussion: In addressing and resolving stakeholder security issues, there are two considerations regarding cyber resiliency. The first is that cyber resiliency issues need to be explicitly considered. The second is that security requirement issues and cyber resiliency requirement issues may be in conflict. For example, from a cyber security perspective, there may be a security requirement to protect internal communications against unauthorized observation. This security requirement translates into a system requirement to encrypt internal communication traffic to counter the threat of data be sniffed and captured by adversaries. From a cyber resiliency perspective, there may be a requirement that the communication traffic remain unencrypted as those encrypted communication flows are often places that the APT employs to hide exfiltration of data or commands from the adversary to the implanted malware.

Table 6 lists the cyber resiliency considerations for the *Stakeholder Needs and Requirements Definition* process.

TABLE 6: CYBER RESILIENCY CONSIDERATIONS FOR STAKEHOLDER NEEDS AND REQUIREMENTS DEFINITION

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
SN-1	PREPARE FOR STAKEHOLDER PROTECTION NEEDS AND SECURITY REQUIREMENTS DEFINITION	No change.
SN-1.1	Identify the stakeholders who have a security interest in the system throughout its life cycle.	Change “security interest” to “security and cyber resiliency interest.”
SN-1.2	Define the stakeholder protection needs and security requirements definition strategy.	Change “security requirements” to “security and cyber resiliency requirements.”
SN-1.3	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of the stakeholder needs and requirements definition process.	Change “security aspects” to “security and cyber resiliency aspects.”
SN-2	DEFINE STAKEHOLDER PROTECTION NEEDS	No change.
SN-2.1	Define the security context of use across all preliminary life cycle concepts.	See Discussion.
SN-2.2	Identify stakeholder assets and asset classes.	No change.
SN-2.3	Prioritize assets based on the adverse consequence of asset loss.	See Discussion.
SN-2.4	Determine asset susceptibility to adversity and uncertainty.	No change.
SN-2.5	Identify stakeholder protection needs.	No change.
SN-2.6	Prioritize and down-select the stakeholder protection needs.	No change.
SN-2.7	Define the stakeholder protection needs and rationale.	See Discussion.

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
SN-3	DEVELOP THE SECURITY ASPECTS OF OPERATIONAL AND OTHER LIFE CYCLE CONCEPTS	Change "security aspects" to "security and cyber resiliency aspects."
SN-3.1	Define a representative set of scenarios to identify all required protection capabilities and security measures that correspond to anticipated operational and other life cycle concepts.	Change "security measures" to "security and cyber resiliency measures."
SN-3.2	Identify the security-relevant interaction between users and the system.	No change.
SN-4	TRANSFORM STAKEHOLDER PROTECTION NEEDS INTO SECURITY REQUIREMENTS	No change.
SN-4.1	Identify the security-oriented constraints on a system solution.	Change "security-oriented constraints" to "security and cyber resiliency-oriented constraints."
SN-4.2	Identify the stakeholder security requirements and security functions.	Change "security requirements" to "security and cyber resiliency requirements." Change "security functions" to "security and cyber resiliency functions."
SN-4.3	Define stakeholder security requirements, consistent with life cycle concepts, scenarios, interactions, constraints, and critical quality characteristics.	Change "security requirements" to "security and cyber resiliency requirements."
SN-4.4	Apply security metadata tagging to identify stakeholder security requirements and security-driven constraints.	No change.
SN-5	ANALYZE STAKEHOLDER SECURITY REQUIREMENTS	No change.
SN-5.1	Analyze the complete set of stakeholder security requirements.	Change "security requirements" to "security and cyber resiliency requirements."
SN-5.2	Define critical security-relevant performance and assurance measures that enable the assessment of technical achievement.	No change.
SN-5.3	Validate that stakeholder protection needs and expectations have been adequately captured and expressed by the analyzed security requirements.	No change.
SN-5.4	Resolve stakeholder security requirements issues.	See Discussion.
SN-6	MANAGE STAKEHOLDER PROTECTION NEEDS AND SECURITY REQUIREMENTS DEFINITION	No change.
SN-6.1	Obtain explicit agreement on the stakeholder security requirements.	Change "security requirements" to "security and cyber resiliency requirements."
SN-6.2	Record asset protection data.	No change.
SN-6.3	Maintain traceability between stakeholder protection needs and stakeholder security requirements.	No change.

3.3 SYSTEM REQUIREMENTS DEFINITION

Cyber Resiliency Engineering Purpose

When considering cyber resiliency as part of the *System Requirements Definition* process, systems security engineering identifies system requirements for cyber resiliency which reflect the identified stakeholder requirements for cyber resiliency. System requirements for cyber resiliency refine and situate stakeholder requirements in the context of cyber resiliency design constraints, which take into consideration the type of system, existing investments in technologies and processes, the intended effects on adversaries, and the maturity of technologies to be included in the system-of-interest. This analysis helps to determine which cyber resiliency techniques and implementation approaches are applicable. System requirements related to cyber resiliency can be expressed in terms of performance measures.

Cyber Resiliency Engineering Outcomes

- Cyber resiliency design constraints are defined.
- Applicable cyber resiliency techniques and approaches are determined.
- Cyber resiliency performance measures are defined.

Cyber Resiliency Considerations

SR-2.2 Define system security **and cyber resiliency** requirements, security **and cyber resiliency** constraints on system requirements, and rationale.

Discussion: From a cyber resiliency perspective, susceptibility to disruption, hazard, and threat should be considered not only with respect to direct consequences, but also to deferred and indirect consequences. Direct consequences disrupt, destroy, disable, or otherwise impact the ability of the system to support the mission or business functions. Deferred consequences include an adversary's establishment of a persistent foothold in the system, enabling the adversary to discover assets and functional dependencies and to plan future attacks. Indirect consequences include consequences at a different scale than the system (e.g., use of the system as a launch pad for attacks on other systems, initiation of cascading failure across a critical infrastructure sector).

SR-3.1 Analyze the complete set of system requirements in consideration of security **and cyber resiliency** concerns.

Discussion: For cyber resiliency, the assumption that an adversary can achieve a persistent foothold in the systems should be explicitly noted.

SR-4.2 Maintain traceability of system security requirements and security- **and cyber resiliency-**driven constraints.

Discussion: From a cyber resiliency perspective, the trustworthiness objectives and loss tolerance should include the cyber resiliency objectives that were identified by the stakeholders. In addition, loss tolerance should consider resiliency unique considerations such as tolerance for training to achieve critical mission and business objectives despite an adversary's malware remaining in the system.

Table 7 lists the cyber resiliency considerations for the *System Requirements Definition* process.

TABLE 7: CYBER RESILIENCY CONSIDERATIONS FOR SYSTEM REQUIREMENTS DEFINITION

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
SR-1	PREPARE FOR SYSTEM SECURITY REQUIREMENTS DEFINITION	No change.
SR-1.1	Define the security aspects of the functional boundary of the system in terms of the security behavior and security properties to be provided.	Change "security properties" to "security and cyber resiliency properties."
SR-1.2	Define the security domains of the system and their correlation to the functional boundaries of the system.	No change.
SR-1.3	Define the security aspects of the system requirements definition strategy.	Change "security aspects" to "security and cyber resiliency aspects."
SR-1.4	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of the system requirements definition process.	Change "security aspects" to "security and cyber resiliency aspects."
SR-2	DEFINE SYSTEM SECURITY REQUIREMENTS	No change.
SR-2.1	Define each security function that the system is required to perform.	Change "security function" to "security and cyber resiliency function."
SR-2.2	Define system security requirements, security constraints on system requirements, and rationale.	Change "security" to "security and cyber resiliency." See Discussion.
SR-2.3	Incorporate system security requirements and associated constraints into system requirements and define rationale.	Change "security requirements" to "security and cyber resiliency requirements."
SR-2.4	Apply security metadata tagging to identify system security requirements and security-driven constraints.	Change "security-driven constraints" to "security and cyber resiliency-driven constraints."
SR-3	ANALYZE SYSTEM SECURITY IN SYSTEM REQUIREMENTS	No change.
SR-3.1	Analyze the complete set of system requirements in consideration of security concerns.	Change "security concerns" to "security and cyber resiliency concerns." See Discussion.
SR-3.2	Define security-driven performance and assurance measures that enable the assessment of technical achievement.	Change "security-driven" to "security and cyber resiliency-driven."
SR-3.3	Provide the analyzed system security requirements and security-driven constraints to applicable stakeholders for review.	Change "security requirements" to "security and cyber resiliency requirements." Change "security-driven constraints" to "security and cyber resiliency-driven constraints."
SR-3.4	Resolve system security requirements and security-driven constraints issues.	Change "security requirements" to "security and cyber resiliency requirements." Change "security-driven constraints" to "security and cyber resiliency-driven constraints."
SR-4	MANAGE SYSTEM SECURITY REQUIREMENTS	No change.
SR-4.1	Obtain explicit agreement on the system security requirements and security-driven constraints.	Change "security requirements" to "security and cyber resiliency requirements." Change "security-driven constraints" to "security and cyber resiliency-driven constraints."

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
SR-4.2	Maintain traceability of system security requirements and security-driven constraints.	See Discussion.
SR-4.3	Provide security-relevant information items required for systems requirements definition to baselines.	No change.

3.4 ARCHITECTURE DEFINITION

Cyber Resiliency Engineering Purpose

When considering cyber resiliency as part of the *Architecture Definition* process, systems security engineering generates cyber resiliency views of the system architecture alternatives to guide and inform the selection of one or more alternatives. These cyber resiliency views may be integrated into security views, or may be presented separately. In addition, systems security engineering ascertains that cyber resiliency analytic processes have been applied across all representative architecture views, to identify functional and assurance dependencies, as well as potential consequences of exploitation of vulnerabilities and susceptibilities identified from security engineering analysis. Cyber resiliency analyses of system architectural views, particularly of security views, inform multiple types of risk assessments (including programmatic; system security; mission, business, or operational; and organizational), risk treatment, and engineering decision making and trades. This process is fully synchronized with the *System Requirements Definition* and *Design Definition* processes, and iterates with the *Business and Mission Analysis* and *Stakeholder Needs and Requirements Definition* processes, in order to achieve a negotiated understanding of the relative priorities of cyber resiliency goals, objectives, methods, capabilities, and design principles, and the constraints on selecting and applying cyber resiliency techniques and approaches. This process also employs the *System Analysis* process to conduct cyber resiliency analyses of the system and architectural alternatives.

Cyber Resiliency Engineering Outcomes

- Cyber resiliency concerns of stakeholders are addressed by the architecture.
- The relevant strategic cyber resiliency design principles are embodied in the architecture.
- The perspective that the adversary may achieve a persistent foothold in the system and an architecture should be designed to address that concern is reflected in the concept of secure function for the system.
- Cyber resiliency structural design principles, techniques, and approaches are allocated to architectural elements, consistent with strategic design principles.
- Security viewpoints, views, and models of the system architecture incorporate cyber resiliency and threat-informed constructs.

Cyber Resiliency Considerations

AR-2.1 Define the concept of secure function for the system at the architecture level.

Discussion: From a cyber resiliency perspective, the concept of secure function defines a strategy for achieving cyber resiliency objectives, applying cyber resiliency design principles, and using cyber resiliency techniques and approaches, consistent with and integrated with the strategy for system security.

The concept of secure function encompasses various security design principles which are closely related to cyber resiliency design principles, including for example: separation; isolation; encapsulation; non-bypassability; layering; modularity; hierarchical trust; hierarchical protection; and secure distributed composition. To incorporate a cyber resiliency perspective, relevant strategic cyber resiliency design principles (Section 2.2.4 and Appendix F.1) are used to guide analysis of architectural alternatives, and to select relevant structural cyber resiliency design principles (Appendix F.2).

AR-2.2 Select, adapt, or develop the security viewpoints and model kinds based on stakeholder security **and cyber resiliency** concerns.

Discussion: A security view which explicitly takes a cyber resiliency perspective, includes the results of analyzing the architecture with respect to relevant strategic cyber resiliency design principles; identifies relevant structural cyber resiliency design principles; and enables the architecture and subsequently the design to be analyzed with respect to where and how well those principles are applied. From the standpoint of cyber resiliency, a security viewpoint should include a representation of critical mission or business process flows, as well as of control flows that include critical security functionality. The kinds of models should include cyber resiliency models.

AR-2.3 Identify the security architecture frameworks to be used in developing the security **and cyber resiliency** models and security **and cyber resiliency** views of the system architecture.

Discussion: Security architecture frameworks which can be used in developing cyber resiliency models and views are extensible or mappable to frameworks used in cyber resiliency modeling. Frameworks used in cyber resiliency modeling include the conceptual cyber resiliency engineering framework introduced in Section 2.2, as well as frameworks that reflect an adversarial perspective. Examples of such frameworks include taxonomies of threat events as in [NIST 800-30], the ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework (as discussed in Appendix J), and other cyber-attack life cycle or cyber kill chain modeling frameworks; and frameworks for describing effects on threat events (as discussed in Appendix I).

AR-3.6 Harmonize the security **and cyber resiliency** models and **the** security **and cyber resiliency** views with each other and with the concept of secure function.

Discussion: Harmonization of security and cyber resiliency models focuses on ensuring consistency of the modeled emergent behavior of the system. In addition, harmonization can map functional capabilities represented by different models. For example, a cybersecurity model that focuses on how "identify, protect, detect, respond, and recover" [NIST CSF] are achieved can be aligned with a cyber resiliency model that represents how the cyber resiliency objectives are achieved.

AR-4.5 Define the security **and cyber resiliency** design principles for the system design and evolution that reflect the concept of secure function.

Discussion: The cyber resiliency design principles (Section 3.1.4 and Appendix F) are considered in this task, with emphasis on those cyber resiliency design principles which are included explicitly to address the APT (e.g., Expect adversaries to evolve; Change or disrupt attack surface).

Table 8 lists the cyber resiliency considerations for the *Architecture Definition* process.

TABLE 8: CYBER RESILIENCY CONSIDERATIONS FOR ARCHITECTURE DEFINITION

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
AR-1	PREPARE FOR ARCHITECTURE DEFINITION FROM THE SECURITY VIEWPOINT	No change.
AR-1.1	Identify the key drivers that impact the security aspects of the system architecture.	Change "impact the security aspects" to "impact the security and cyber resiliency aspects."

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
AR-1.2	Identify stakeholder security concerns.	Change "security" to "security and cyber resiliency."
AR-1.3	Define the security aspects of the architecture definition roadmap, approach, and strategy.	Change "security" to "security and cyber resiliency."
AR-1.4	Define evaluation criteria based on stakeholder security concerns and security-relevant requirements.	Change "security concerns" to "security and cyber resiliency concerns."
AR-1.5	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of the architecture definition process.	Change "security" to "security and cyber resiliency."
AR-2	DEVELOP SECURITY VIEWPOINTS OF THE ARCHITECTURE	No change.
AR-2.1	Define the concept of secure function for the system at the architecture level.	See Discussion.
AR-2.2	Select, adapt, or develop the security viewpoints and model kinds based on stakeholder security concerns.	Change "security concerns" to "security and cyber resiliency concerns." See Discussion.
AR-2.3	Identify the security architecture frameworks to be used in developing the security models and security views of the system architecture.	Change "security models" to "security and cyber resiliency models." Change "security views" to "security and cyber resiliency views." See Discussion.
AR-2.4	Record the rationale for the selection of architecture frameworks that address security concerns, security viewpoints, and security model types.	Change "security" to "security and cyber resiliency."
AR-2.5	Select or develop supporting security modeling techniques and tools.	Change "security" to "security and cyber resiliency."
AR-3	DEVELOP SECURITY MODELS AND SECURITY VIEWS OF CANDIDATE ARCHITECTURES	Change "security" to "security and cyber resiliency."
AR-3.1	Define the security context and boundaries of the system in terms of interfaces, interconnections, and interactions with external entities.	No change.
AR-3.2	Identify architectural entities and relationships between entities that address key stakeholder security concerns and system security requirements.	Change "security concerns" to "security and cyber resiliency concerns."
AR-3.3	Allocate security concepts, properties, characteristics, behavior, functions, or constraints to architectural entities.	Change "security" to "security and resiliency."
AR-3.4	Select, adapt, or develop security models of the candidate architectures.	Change "security models" to "security and cyber resiliency models."
AR-3.5	Compose views in accordance with security viewpoints to express how the architecture addresses stakeholder security concerns and meets stakeholder and system security requirements.	Change "security viewpoints" to "security and resiliency viewpoints." Change "security concerns" to "security and resiliency concerns."
AR-3.6	Harmonize the security models and security views with each other and with the concept of secure function.	Change "security" to "security and cyber resiliency." See Discussion.

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
AR-4	RELATE SECURITY VIEWS OF THE ARCHITECTURE TO DESIGN	No change.
AR-4.1	Identify the security-relevant system elements that relate to architectural entities and the nature of these relationships.	Change “security-relevant system elements” to “security and cyber resiliency-relevant system elements.”
AR-4.2	Define the security interfaces, interconnections, and interactions between the system elements and with external entities.	No change.
AR-4.3	Allocate system security requirements to architectural entities and system elements.	Change “system security requirements” to “system security and cyber resiliency requirements.”
AR-4.4	Map security-relevant system elements and architectural entities to security design characteristics.	Change “security-relevant” to “security and cyber resiliency-relevant.” Change “security design” to “security and cyber resiliency design.”
AR-4.5	Define the security design principles for the system design and evolution that reflect the concept of secure function.	Change “security design” to “security and cyber resiliency design.” See Discussion.
AR-5	SELECT CANDIDATE ARCHITECTURE	No change.
AR-5.1	Assess each candidate architecture against the security requirements and security-related constraints.	Change “security requirements” to “security and cyber resiliency requirements.” Change “security-related” to “security and cyber resiliency-related.”
AR-5.2	Assess each candidate architecture against stakeholder security concerns using evaluation criteria.	Change “security concerns” to “security and cyber resiliency concerns.” See Discussion.
AR-5.3	Select the preferred architecture(s) and capture key security decisions and rationale for those decisions.	Change “security decisions” to “security and cyber resiliency decisions.”
AR-5.4	Establish the security aspects of the architecture baseline of the selected architecture.	Change “security aspects” to “security and cyber resiliency aspects.”
AR-6	MANAGE THE SECURITY VIEW OF THE SELECTED ARCHITECTURE	No change.
AR-6.1	Formalize the security aspects of the architecture governance approach and specify security governance-related roles and responsibilities, accountabilities, and authorities.	Change “security aspects” to “security and cyber resiliency aspects.”
AR-6.2	Obtain explicit acceptance of the security aspects of the architecture by stakeholders.	Change “security aspects” to “security and cyber resiliency aspects.”
AR-6.3	Maintain concordance and completeness of the security architectural entities and their security-related architectural characteristics.	Change “security architectural” to “security and cyber resiliency architectural.” Change “security-related architectural characteristics” to “security- and cyber resiliency-related architectural characteristics.”
AR-6.4	Organize, assess, and control the evolution of the security models and security views of the architecture.	Change “security models” to “security and cyber resiliency models.”

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
AR-6.5	Maintain the security aspects of the architecture definition and evaluation strategy.	Change "security aspects" to "security and cyber resiliency aspects."
AR-6.6	Maintain traceability of the security aspects of the architecture.	Change "security aspects" to "security and cyber resiliency aspects."
AR-6.7	Provide security-relevant information items required for architecture definition to baselines.	Change "security-relevant" to "security and cyber resiliency-relevant."

3.5 DESIGN DEFINITION

Cyber Resiliency Engineering Purpose

When considering cyber resiliency as part of the *Design Definition* process, systems security engineering considers cyber resiliency design characteristics as well as, and in close relationship with, security design characteristics. Cyber resiliency design characteristics include where and how the relevant cyber resiliency design principles are applied, and how that application relates to the application of relevant security design principles; where and how the potentially applicable techniques, subject to design constraints as determined as part of the *System Requirements Definition* process, are or could be applied.

Cyber Resiliency Engineering Outcomes

- Relevant structural cyber resiliency design principles are identified and interpreted in the context of the architecture and design.
- Technologies to support the application of cyber resiliency design principles are identified.

Cyber Resiliency Considerations

DE-1.1 Apply the concept of secure function for the system at the design level.

Discussion: The concept of secure function encompasses security design principles and concepts. Examples include: separation; isolation; encapsulation; least privilege; modularity; non-bypassability; layering; hierarchical trust; hierarchical protection; and secure distributed composition. From a cyber resiliency perspective, the various structural cyber resiliency design principles described in Appendix F.2 and determined to be relevant based on the constraints identified as part of the *Systems Requirements Definition* process are considered as well. Synergies and interactions among cyber resiliency design principles, and between cyber resiliency design principles and security design principles, are identified and analyzed.

DE-1.2 Determine the security technologies required for each system element composing the system.

Discussion: Examples of security technologies include: cryptography; secure operating systems, virtual machines, and hypervisors; identity and strong authentication; domain perimeter, domain separation, and cross-domain technologies; security instrumentation and monitoring; physical and electronic tamper protection; and protection against reverse engineering. From a cyber resiliency perspective, such techniques as Deception (e.g., honeynets), Architectural Diversity, Design Diversity, Non-Persistent Information, Dynamic Positioning (e.g., relocation of assets, fragmenting information), Non-Persistent Services, and Unpredictability are considered, subject to the constraints identified as part of the *Systems Requirements Definition* process. These techniques and approaches are intended to address adversarial threat events in general and the APT, in particular.

DE-1.4 Define the principles for secure evolution of the system design.

Discussion: From a cyber resiliency perspective, the principles for secure evolution of the system design reflect the cyber resiliency goal of Adapt and the cyber resiliency objective of Re-Architect, subject to the relative priorities expressed by stakeholders. The cited goal and objective are intended to ensure that the system can adapt in the face of yet unseen adversarial threats. The principles for secure evolution of the system design can include concepts for use of systems or services in the environment of operations, as new capabilities are offered by such systems or services. For example, using a service that facilitates an ability to refresh the system or system elements (e.g., including a virtualization capability) would facilitate the Maximize transience design principle as well as the Change or disrupt attack surface design principle.

DE-1.6 Identify, plan for, and obtain access to enabling systems or services to support the security aspects of the design definition process.

Discussion: From a cyber resiliency perspective, enabling systems or services extend the attack surface of the system-of-interest.

DE-2.2 Transform security architectural characteristics into security design characteristics.

Discussion: An important security objective of system design is to avoid vulnerability where possible, and to minimize, manage, and mitigate vulnerability otherwise. From a cyber resiliency perspective, that is a necessary, but not necessarily sufficient objective. Systems are very complex entities and as such, it is not possible to eliminate all vulnerabilities. Therefore, adversaries will be given many opportunities to exploit unmitigated known and unknown vulnerabilities. From a cyber resiliency perspective, the design should facilitate redirecting the adversary, precluding adversary activities, impeding the adversary, limiting the adversary, and exposing the adversary.

Table 9 lists the cyber resiliency considerations for the *Design Definition* process.

TABLE 9: CYBER RESILIENCY CONSIDERATIONS FOR DESIGN DEFINITION

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
DE-1	PREPARE FOR SECURITY DESIGN DEFINITION	No change.
DE-1.1	Apply the concept of secure function for the system at the design level.	See Discussion.
DE-1.2	Determine the security technologies required for each system element composing the system.	See Discussion.
DE-1.3	Determine the types of security design characteristics.	No change.
DE-1.4	Define the principles for secure evolution of the system design.	See Discussion.
DE-1.5	Define the security aspects of the design definition strategy.	No change.
DE-1.6	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of the design definition process.	See Discussion.
DE-2	ESTABLISH SECURITY DESIGN CHARACTERISTICS AND ENABLERS FOR EACH SYSTEM ELEMENT	No change.
DE-2.1	Allocate system security requirements to system elements.	Change “system security requirements” to “system security and cyber resiliency requirements.”
DE-2.2	Transform security architectural characteristics into security design characteristics.	See Discussion.

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
DE-2.3	Define the necessary security design enablers.	Change "security design enablers" to "security and cyber resiliency design enablers." Cyber resiliency design enablers include cyber resiliency models and modeling techniques.
DE-2.4	Examine security design alternatives.	Change "security design alternatives" to "security and cyber resiliency design alternatives."
DE-2.5	Refine or define the security interfaces between the system elements and with external entities.	No change.
DE-2.6	Develop the security design artifacts.	Change "security design artifacts" to "security and cyber resiliency design artifacts."
DE-3	ASSESS THE ALTERNATIVES FOR OBTAINING SECURITY-RELEVANT SYSTEM ELEMENTS	No change.
DE-3.1	Identify security-relevant nondevelopmental items (NDI) that may be considered for use.	No change.
DE-3.2	Assess each candidate NDI and new design alternative against the criteria developed from expected security design characteristics or system element security requirements to determine suitability for the intended application.	No change.
DE-3.3	Determine the preferred alternative among candidate NDI solutions and new design alternatives for a system element.	No change.
DE-4	MANAGE THE SECURITY DESIGN	No change.
DE-4.1	Map the security design characteristics to the system elements.	Change "security design characteristics" to "security design and cyber resiliency characteristics."
DE-4.2	Capture the security design and rationale.	Change "security design" to "security and cyber resiliency design."
DE-4.3	Maintain traceability of the security aspects of the system design.	No change.
DE-4.4	Provide security-relevant information items required for the system design definition to baselines.	Change "security-relevant" to "security and cyber resiliency relevant."

3.6 SYSTEM ANALYSIS

Cyber Resiliency Engineering Purpose

As part of the *System Analysis* process, systems security engineering addresses cyber resiliency aspects of analysis, which include representation of the assumption that the adversary may be able to achieve a persistent foothold in the system, and can include identification of the extent to which classes of threat events or examples of specific threat events are used in analysis, the extent to which effects of alternative design decisions or cyber resiliency solutions on threat events are analyzed, and which forms of cyber resiliency behavioral modeling (if any) are used. (See Section

2.5 for more information on analytic methods for cyber resiliency.) Functional dependencies of cyber resiliency capabilities on underlying security capabilities are identified, to determine the potential consequences of misuse or failure of security functionality.

Cyber Resiliency Engineering Outcomes

- Cyber resiliency analysis objectives are articulated, including their relationship to security analysis objectives.
- Cyber resiliency assumptions, especially those regarding the nature and capability of the adversary and the classes of threat events to be considered, are articulated.
- The dependency of cyber resiliency functionality on underlying security functionality is identified.

Cyber Resiliency Considerations

SA-1.3 Define the objectives, scope, level of fidelity, and level of assurance of the security **and cyber resiliency** aspects of system analysis.

Discussion: From a cyber resiliency perspective, the objectives of system analysis can include, for example, identification of the extent to which relevant cyber resiliency design principles have been applied; the level of confidence that a given design principle has been applied effectively; the classes of threat events which are addressed by the system; and how and how well the system addresses a given class of threat events. The scope of system analysis can be restricted to the system-of-interest, or specific elements of the system-of-interest; it can also be extended to include enabling systems and other systems in the environment of operations. From a cyber resiliency perspective, enabling systems and other systems in the environment of operations extend the attack surface of the system-of-interest. In addition, the consequences of threat events on the system-of-interest can result in consequences to other systems in the environment of operations (e.g., attack propagation, cascading failure). The minimum acceptable level of fidelity for metrics or measures of effectiveness related to achieving cyber resiliency objectives or meeting cyber resiliency requirements is defined.

SA-1.5 Define the security **and cyber resiliency** aspects of the system analysis strategy.

Discussion: The importance of dependency analysis is noted in [NIST 800-160, Vol. 1]. From a cyber resiliency perspective, the dependency analysis should also examine the dependency of cyber resiliency objectives and functions on their corresponding security objectives and functions.

SA-2.1 Identify and validate the assumptions associated with the security **and cyber resiliency** aspects of system analysis.

Discussion: From a cyber resiliency perspective, one of the critical assumptions is that the adversary will be able to circumvent boundary protection measures and achieve a persistent foothold in the system, will evolve, and will continually attempt to achieve its goals. The nature of the APT is such that the ability to validate such assumptions will be challenging, and it may not be possible to remove uncertainty about the assumptions.

Table 10 lists the cyber resiliency considerations for the *System Analysis* process.

TABLE 10: CYBER RESILIENCY CONSIDERATIONS FOR SYSTEM ANALYSIS

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
SA-1	PREPARE FOR THE SECURITY ASPECTS OF SYSTEM ANALYSIS	No change.

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
SA-1.1	Identify the security aspects of the problem or question that requires system analysis.	Change "security aspects" to "security and cyber resiliency aspects."
SA-1.2	Identify the stakeholders of the security aspects of system analysis.	Change "security aspects" to "security and cyber resiliency aspects."
SA-1.3	Define the objectives, scope, level of fidelity, and level of assurance of the security aspects of system analysis.	See Discussion.
SA-1.4	Select the methods associated with the security aspects of system analysis.	Change "security aspects" to "security and cyber resiliency aspects."
SA-1.5	Define the security aspects of the system analysis strategy.	Change "security aspects" to "security and cyber resiliency aspects." See Discussion.
SA-1.6	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of the system analysis process.	Change "security aspects" to "security and cyber resiliency aspects."
SA-1.7	Collect the data and inputs needed for the security aspects of system analysis.	Change "security aspects" to "security and cyber resiliency aspects."
SA-2	PERFORM THE SECURITY ASPECTS OF SYSTEM ANALYSIS	No change.
SA-2.1	Identify and validate the assumptions associated with the security aspects of system analysis.	See Discussion.
SA-2.2	Apply the selected security analysis methods to perform the security aspects of required system analysis.	Change "security aspects" to "security and cyber resiliency aspects."
SA-2.3	Review the security aspects of the system analysis results for quality and validity.	Change "security aspects" to "security and cyber resiliency aspects."
SA-2.4	Establish conclusions, recommendations, and rational based on the results of the security aspects of system analysis.	Change "security aspects" to "security and cyber resiliency aspects."
SA-2.5	Record the results of the security aspects of system analysis.	Change "security aspects" to "security and cyber resiliency aspects."
SA-3	MANAGE THE SECURITY ASPECTS OF SYSTEM ANALYSIS	No change.
SA-3.1	Maintain traceability of the security aspects of the system analysis results.	Change "security aspects" to "security and cyber resiliency aspects."
SA-3.2	Provide security-relevant system analysis information items that have been selected for baselines.	Change "security-relevant" to "security and cyber resiliency relevant."

3.7 IMPLEMENTATION

Cyber Resiliency Engineering Purpose

When considering cyber resiliency as part of the *Implementation* process, systems security engineering focuses on the security aspects of system elements and of the implementation strategy, so that cyber resiliency is not a direct consideration. However, the implementation

strategy must ensure that the properties and protection capabilities of system elements are provided in such a way as to meet cyber resiliency needs and achieve cyber resiliency objectives.

Cyber Resiliency Engineering Outcomes

- The security aspects of implementation that constrain the ability to achieve cyber resiliency objectives or to meet cyber resiliency needs are identified.

Cyber Resiliency Considerations

IP-1.2 Identify constraints from the security aspects of the implementation strategy and technology on the system requirements, architecture, design, or implementation techniques.

Discussion: The security aspects of the implementation strategy oriented toward the specific choice of implementation technology or the manner in which the system element is to be realized, may impose constraints on the selection of cyber resiliency techniques, approaches, or solutions, and ultimately on the ability to achieve cyber resiliency objectives or meet cyber resiliency needs. Identification of these constraints is crucial to guiding and informing engineering trade-offs.

Table 11 lists the cyber resiliency considerations for the *Implementation* process.

TABLE 11: CYBER RESILIENCY CONSIDERATIONS FOR IMPLEMENTATION

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
IP-1	PREPARE FOR THE SECURITY ASPECTS OF IMPLEMENTATION	No change.
IP-1.1	Develop the security aspects of the implementation strategy.	No change.
IP-1.2	Identify constraints from the security aspects of the implementation strategy and technology on the system requirements, architecture, design, or implementation techniques.	See Discussion.
IP-1.3	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of implementation.	No change.
IP-2	PERFORM THE SECURITY ASPECTS OF IMPLEMENTATION	No change.
IP-2.1	Realize or adapt system elements in accordance with the security aspects of the implementation strategy, defined implementation procedures, and security-driven constraints.	No change.
IP-2.2	Develop initial training materials for users for operation, sustainment, and support.	No change.
IP-2.3	Securely package and store system elements.	No change.
IP-2.4	Record evidence that system elements meet the system security requirements.	No change.
IP-3	MANAGE RESULTS OF THE SECURITY ASPECTS OF IMPLEMENTATION	No change.
IP-3.1	Record the security aspects of implementation results and any security-related anomalies encountered.	No change.
IP-3.2	Maintain traceability of the security aspects of implemented system elements.	No change.

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
IP-3.3	Provide security-relevant information items required for implementation to baselines.	No change.

3.8 INTEGRATION

Cyber Resiliency Engineering Purpose

No change from Systems Security Engineering Purpose.

Cyber Resiliency Engineering Outcomes

No change from Systems Security Engineering Outcomes.

Cyber Resiliency Considerations

Table 12 lists the cyber resiliency considerations for the *Integration* process.

TABLE 12: CYBER RESILIENCY CONSIDERATIONS FOR INTEGRATION

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
IN-1	PREPARE FOR THE SECURITY ASPECTS OF INTEGRATION	No change.
IN-1.1	Identify and define checkpoints for the trustworthy secure operation of the assembled interfaces and selected system functions.	No change.
IN-1.2	Develop the security aspects of the integration strategy.	Change “security aspects” to “security and cyber resiliency aspects.”
IN-1.3	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of integration.	Change “security aspects” to “security and cyber resiliency aspects.”
IN-1.4	Identify the constraints resulting from the security aspects of integration to be incorporated into the system requirements, architecture, or design.	Change “security aspects” to “security and cyber resiliency aspects.”
IN-2	PERFORM THE SECURITY ASPECTS OF INTEGRATION	No change.
IN-2.1	Obtain implemented system elements in accordance with security criteria and requirements established in agreements and schedules.	Change “security criteria and requirements” to “security and cyber resiliency criteria and requirements.”
IN-2.2	Assemble the implemented system elements to achieve secure configurations.	No change.
IN-2.3	Perform checks of the security characteristics of interfaces, functional behavior, and behavior across interconnections.	Change “security characteristics” to “security and cyber resiliency characteristics.”
IN-3	MANAGE RESULTS OF THE SECURITY ASPECTS OF INTEGRATION	No change.
IN-3.1	Record the security aspects of integration results and any security anomalies encountered.	Change “security aspects” to “security and cyber resiliency aspects.”

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
		Change "security anomalies" to "security and cyber resiliency anomalies."
IN-3.2	Maintain traceability of the security aspects of integrated system elements.	Change "security aspects" to "security and cyber resiliency aspects."
IN-3.3	Provide security-relevant information items required for integration to baselines.	Change "security relevant" to "security and cyber resiliency relevant."

3.9 VERIFICATION

Cyber Resiliency Engineering Purpose

When considering cyber resiliency as part of the *Verification* process, systems security engineering produces evidence that the system satisfies its cyber resiliency-relevant system requirements and has its required cyber resiliency characteristics. (See Section 2.3.2 for discussion of requirements, characteristics, and aspects of the verification strategy.)

Cyber Resiliency Engineering Outcomes

- The cyber resiliency aspects of the verification strategy are developed.
- Any enabling systems or services needed to achieve the cyber resiliency aspects of the verification strategy are available.

Cyber Resiliency Considerations

VE-2.1 Define the security **and cyber resiliency** aspects of the verification procedures, each supporting one or a set of security- **and cyber resiliency**-focused verification actions.

Discussion: Verification procedures related to cyber resiliency focus on cyber resiliency capabilities in the context of mission or business process objectives, and under the assumption of adversary compromise of system elements. The procedures identify the tailored cyber resiliency objectives and the cyber resiliency criteria for acceptance.

VE-2.2 Perform security **and cyber resiliency** verification procedures.

Discussion: Cyber resiliency verification, like security verification, can be performed at multiple points in the system life cycle. Modeling and simulation, or model-based systems engineering, methods to evaluate correctness can be used before a system element is implemented, based on design artifacts. Cyber resiliency verification does not typically search for vulnerabilities, but can include examining interactions between system elements which could result in cascading failures, propagation of malware or incorrect data, or the ripple effects of threat events.

Table 13 lists the cyber resiliency considerations for the *Verification* process.

TABLE 13: CYBER RESILIENCY CONSIDERATIONS FOR VERIFICATION

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
VE-1	PREPARE FOR THE SECURITY ASPECTS OF VERIFICATION	Change "security aspects" to "security and cyber resiliency aspects."

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
VE-1.1	Identify the security aspects within the verification scope and corresponding security-focused verification actions.	Change "security aspects" to "security and cyber resiliency aspects." Change "security-focused verification actions" to "verification actions focused on security and cyber resiliency."
VE-1.2	Identify the constraints that can potentially limit the feasibility of the security-focused verification actions.	Change "security-focused verification actions" to "verification actions focused on security and cyber resiliency."
VE-1.3	Select the appropriate methods or techniques for the security aspects of verification and the associated security criteria for each security-focused verification action.	Change "security aspects" to "security and cyber resiliency aspects." Change "security-focused verification actions" to "verification actions focused on security and cyber resiliency."
VE-1.4	Define the security aspects of the verification strategy.	Change "security aspects" to "security and cyber resiliency aspects."
VE-1.5	Identify the system constraints resulting from the security aspects of the verification strategy to be incorporated into the system requirements, architecture, or design.	Change "security aspects" to "security and cyber resiliency aspects."
VE-1.6	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of verification.	Change "security aspects" to "security and cyber resiliency aspects."
VE-2	PERFORM SECURITY-FOCUSED VERIFICATION	Change "security-focused verification" to "verification focused on security and cyber resiliency."
VE-2.1	Define the security aspects of the verification procedures, each supporting one or a set of security-focused verification actions.	Change "security aspects" to "security and cyber resiliency aspects." Change "security-focused verification actions" to "verification actions focused on security and cyber resiliency." See Discussion.
VE-2.2	Perform security verification procedures.	Change "security verification" to "security and cyber resiliency verification." See Discussion.
VE-2.3	Analyze security-focused verification results against any established expectations and success criteria.	Change "security-focused verification" to "verification focused on security and cyber resiliency."
VE-3	MANAGE RESULTS OF SECURITY-FOCUSED VERIFICATION	Change "security-focused verification" to "verification focused on security and cyber resiliency."
VE-3.1	Record the security aspects of verification results and any security anomalies encountered.	Change "security aspects" to "security and cyber resiliency aspects."
VE-3.2	Record the security characteristics of operational incidents and problems and track their resolution.	Change "security characteristics" to "security and cyber resiliency characteristics."
VE-3.3	Obtain stakeholder agreement that the system or system element meets the specified system security requirements and characteristics.	Change "security requirements and characteristics" to "security and cyber resiliency requirements and characteristics."

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
VE-3.4	Maintain traceability of the security aspects of verified system elements.	No change.
VE-3.5	Provide security-relevant information items required for verification to baselines.	No change.

3.10 TRANSITION

Cyber Resiliency Engineering Purpose

No change from Systems Security Engineering Purpose.

Cyber Resiliency Engineering Outcomes

- Aspects of the transition strategy that include the cyber resiliency goals and objectives are developed.
- Threat and APT-informed training for all stakeholders, including users, is developed.
- Threat-informed frameworks and self-challenge tools are developed and employed in preparation for validation of the cyber resiliency of the system.

Cyber Resiliency Considerations

TR-1.1 Develop the security aspects of the transition strategy.

Discussion: The security aspects of transition regarding confidentiality, integrity, availability, and accountability are discussed in [NIST 800-160, Vol. 1]. From a cyber resiliency perspective, the security aspects of transition should also consider the cyber resiliency goals (e.g., ability to Withstand) and objectives (e.g., ability to Constrain).

TR-1.4 Identify and arrange the training necessary for secure system utilization, sustainment, and support.

Discussion: Transition is a perfect opportunity for an adversary to attempt to compromise a system, as it is not fully functioning and thus unable to protect itself. Therefore, the training necessary for transition should also include training about the APT, what to look for in terms of suspicious activity (indicating corrupted behavior), and other threat-related training.

TR-2.4 Demonstrate proper achievement of the security aspects of system installation.

Discussion: From a cyber resiliency perspective, security aspects of the system installation should also consider cyber resiliency goals, objectives, techniques, and implementation approaches that may be affected during system installation.

TR-2-9 Review the security aspects of the system for operational readiness.

Discussion: To help validate the readiness of the system, the organization may consider complementing penetration testing and vulnerability testing with the use of tools that perform a self-challenge (e.g., Simian Army) and use APT-informed threat frameworks (e.g., [MITRE16]) that highlight possible attack paths of an adversary.

Table 14 lists the cyber resiliency considerations for the *Transition* process.

TABLE 14: CYBER RESILIENCY CONSIDERATIONS FOR TRANSITION

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
TR-1	PREPARE FOR THE SECURITY ASPECTS OF TRANSITION	No change.
TR-1.1	Develop the security aspects of the transition strategy.	See Discussion.
TR-1.2	Identify the facility or site changes needed for security purposes.	No change.
TR-1.3	Identify the constraints resulting from the security aspects of transition to be incorporated into the system requirements, architecture, and design.	No change.
TR-1.4	Identify and arrange the training necessary for secure system utilization, sustainment, and support.	See Discussion.
TR-1.5	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of transition.	No change.
TR-2	PERFORM THE SECURITY ASPECTS OF TRANSITION	No change.
TR-2.1	Prepare the facility or site in accordance with the secure installation requirements.	No change.
TR-2.2	Securely deliver the system for installation.	No change.
TR-2.3	Install the system at its specified location and establish secure interconnections to its environment.	No change.
TR-2.4	Demonstrate proper achievement of the security aspects of system installation.	See Discussion.
TR-2.5	Provide security training for stakeholders that interact with the system.	Change “security training” to “security and cyber resiliency training.”
TR-2.6	Perform activation and checkout of the security aspects of the system.	Change “security aspects” to “security and cyber resiliency aspects.”
TR-2.7	Demonstrate that the installed system is capable of delivering the required protection capability.	No change.
TR-2.8	Demonstrate that the security functions provided by the system are sustainable by the enabling systems.	No change.
TR-2.9	Review the security aspects of the system for operational readiness.	See Discussion.
TR-2.10	Commission the system for secure operation.	No change.
TR-3	MANAGE RESULTS OF THE SECURITY APECTS OF TRANSITION	No change.
TR-3.1	Record the security aspects of transition results and any security anomalies encountered.	No change.
TR-3.2	Record the security aspects of operational incidents and problems and track their resolution.	Change “security aspects” to “security and cyber resiliency aspects.”
TR-3.3	Maintain traceability of the security aspects of transitioned system elements.	No change.
TR-3.4	Provide security-relevant information items required for transition to baselines.	No change.

3.11 VALIDATION

Cyber Resiliency Engineering Purpose

When considering cyber resiliency as part of the *Validation* process, systems security engineering produces evidence that the system fulfills its business or mission objectives by satisfying its cyber resiliency-relevant stakeholder requirements and demonstrating its required cyber resiliency characteristics. (See Section 2.3.2 for discussion of requirements, characteristics, and aspects of the validation strategy.)

Cyber Resiliency Engineering Outcomes

- The cyber resiliency aspects of the validation strategy are developed.
- Any enabling systems or services needed to achieve the cyber resiliency aspects of the validation strategy are available.

Cyber Resiliency Considerations

VA-2.1 Define the security **and cyber resiliency** aspects of the validation procedures, each supporting one or a set of security- **and cyber resiliency**-focused validation actions.

Discussion: Validation procedures related to cyber resiliency focus on cyber resiliency capabilities in the context of mission or business process objectives, and under the assumption of adversary compromise of system elements or of other systems. The procedures identify the tailored cyber resiliency objectives; describe how cyber courses of action will be selected and represented in the validation procedures; and identify the cyber resiliency criteria for acceptance. A validation procedure focused on cyber resiliency is targeted toward the system as a whole, or toward critical mission or business functions.

VA-2.2 Perform security **and cyber resiliency** validation procedures in the defined environment.

Discussion: Cyber resiliency validation, like security validation, can be performed at multiple points in the system life cycle. Validation procedures can be executed in a laboratory, testbed, or cyber range, as well as in an operational environment. Cyber resiliency validation can include examining interactions between system elements, or between the system-of-interest and other systems, which could result in cascading failures, propagation of malware or incorrect data, or ripple effects of threat events.

Table 15 lists the cyber resiliency considerations for the *Validation* process.

TABLE 15: CYBER RESILIENCY CONSIDERATIONS FOR VALIDATION

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
VA-1	PREPARE FOR THE SECURITY ASPECTS OF VALIDATION	Change “security aspects” to “security and cyber resiliency aspects.”
VA-1.1	Identify the security aspects of the validation scope and corresponding security-focused validation actions.	Change “security aspects” to “security and cyber resiliency aspects.” Change “security-focused validation actions” to “validation actions focused on security and cyber resiliency.”
VA-1.2	Identify the constraints that can potentially limit the feasibility of the security-focused validation actions.	Change “security-focused validation actions” to “validation actions focused on security and cyber resiliency.”
VA-1.3	Select the appropriate methods or techniques for the security aspects of validation and the	Change “security aspects” to “security and cyber resiliency aspects.”

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
	associated security criteria for each security-focused validation action.	Change "security-focused validation actions" to "validation actions focused on security and cyber resiliency."
VA-1.4	Develop the security aspects of the validation strategy.	Change "security aspects" to "security and cyber resiliency aspects."
VA-1.5	Identify system constraints resulting from the security aspects of validation to be incorporated into the stakeholder security requirements.	Change "security aspects" to "security and cyber resiliency aspects."
VA-1.6	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of validation.	Change "security aspects" to "security and cyber resiliency aspects."
VA-2	PERFORM SECURITY-FOCUSED VALIDATION	Change "security-focused validation" to "validation focused on security and cyber resiliency."
VA-2.1	Define the security aspects of the validation procedures, each supporting one or a set of security-focused validation actions.	Change "security aspects" to "security and cyber resiliency aspects." Change "security-focused validation actions" to "validation actions focused on security and cyber resiliency." See Discussion.
VA-2.2	Perform security validation procedures in the defined environment.	Change "security validation" to "security and cyber resiliency validation." See Discussion.
VA-2.3	Review security-focused validation results to confirm that the protection services of the system that are required by stakeholders are available.	Change "security-focused validation" to "validation focused on security and cyber resiliency."
VA-3	MANAGE RESULTS OF SECURITY-FOCUSED VALIDATION	Change "security-focused validation" to "validation focused on security and cyber resiliency."
VA-3.1	Record the security aspects of validation results and any security anomalies encountered.	Change "security aspects" to "security and cyber resiliency aspects."
VA-3.2	Record the security characteristics of operational incidents and problems and track their resolution.	Change "security characteristics" to "security and cyber resiliency characteristics."
VA-3.3	Obtain stakeholder agreement that the system or system element meets the stakeholder protection needs.	Change "security requirements and characteristics" to "security and cyber resiliency requirements and characteristics."
VA-3.4	Maintain traceability of the security aspects of validated system elements.	No change.
VA-3.5	Provide security-relevant information items required for validation to baselines.	No change.

3.12 OPERATION

Cyber Resiliency Engineering Purpose

When considering cyber resiliency for the *Operation* process, systems security engineering ensures that the operation strategy includes cyber resiliency aspects. The cyber resiliency aspects of the operation strategy focus on ensuring that business or mission objectives are achieved, and

can make explicit, how trade-offs between the execution of business or mission tasks, security, safety, privacy, and other aspects of trustworthiness are made in the operational environment, under different circumstances.

Cyber Resiliency Engineering Outcomes

- The cyber resiliency aspects of the operation strategy are developed.

Cyber Resiliency Considerations

OP-1.1 Develop the security **and cyber resiliency** aspects of the operation strategy.

Discussion: The cyber resiliency aspects of the operation strategy ensure that business or mission objectives can be achieved by using the cyber resiliency capabilities of the system, in conjunction with capabilities of other systems with which the system-of-interest interacts or on which it depends; and that the system's security services are resilient. The cyber resiliency aspects of service availability include consideration of how service priorities change in response to identified business or mission operations or environmental factors. The cyber resiliency aspects of the operation strategy are closely related to contingency and continuity-of-operations planning at the business or mission process level and the organizational level. Information provided by implementing the Analytic Monitoring and Dynamic Representation techniques support gaining insight into performance levels and are central to monitoring changes in hazards and threats. From a cyber resiliency perspective, the operation strategy describes how the Prevent/Avoid, Prepare, Continue, and Constrain cyber resiliency objectives are achieved in the intended operational environment, and under circumstances which, while not intended, may arise (e.g., changes in mission or business processes or priorities).

Table 16 lists the cyber resiliency considerations for the *Operation* process.

TABLE 16: CYBER RESILIENCY CONSIDERATIONS FOR OPERATION

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
OP-1	PREPARE FOR SECURE OPERATION	No change.
OP-1.1	Develop the security aspects of the operation strategy.	Change "security aspects" to "security and cyber resiliency aspects." See Discussion.
OP-1.2	Identify the constraints resulting from the security aspects of operation to be incorporated into the system requirements, architecture, and design.	Change "security aspects" to "security and cyber resiliency aspects."
OP-1.3	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of operation.	Change "security aspects" to "security and cyber resiliency aspects."
OP-1.4	Identify or define security training and qualification requirements; train and assign personnel needed for system operation.	No change.
OP-2	PERFORM SECURE OPERATION	No change.
OP-2.1	Securely use the system in its intended operational environment.	No change.
OP-2.2	Apply materials and other resources, as required, to operate the system in a secure manner and sustain its security services.	No change.
OP-2.3	Monitor the security aspects of system operation.	No change.

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
OP-2.4	Identify and record when system security performance is not within acceptable parameters.	No change.
OP-2.5	Perform system security contingency operations, if necessary.	No change.
OP-3	MANAGE RESULTS OF SECURE OPERATION	No change.
OP-3.1	Record results of secure operation and any security anomalies encountered.	No change.
OP-3.2	Record the security aspects of operational incidents and problems and track their resolution.	No change.
OP-3.3	Maintain traceability of the security aspects of the operations elements.	No change.
OP-3.4	Provide security-relevant information items required for operation to baselines.	No change.
OP-4	SUPPORT SECURITY NEEDS OF CUSTOMERS	No change.
OP-4.1	Provide security assistance and consultation to customers as requested.	No change.
OP-4.2	Record and monitor requests and subsequent actions for security support.	No change.
OP-4.3	Determine the degree to which the delivered system security services satisfy the needs of the customers.	No change.

3.13 MAINTENANCE

Cyber Resiliency Engineering Purpose

No change from Systems Security Engineering Purpose.

Cyber Resiliency Engineering Outcomes

No change from Systems Security Engineering Outcomes.

Cyber Resiliency Considerations

MA-1.1 Define the security aspects of the maintenance strategy.

Discussion: The security aspects related to replacement can use Architectural Diversity, Design Diversity, and Supply Chain Diversity. The security aspects of the logistics strategy and counterfeit and modification prevention can use Supply Chain Diversity, Integrity Checks, and Provenance Tracking.

Table 17 lists the cyber resiliency considerations for the *Maintenance* process.

TABLE 17: CYBER RESILIENCY CONSIDERATIONS FOR MAINTENANCE

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
MA-1	PREPARE FOR THE SECURITY ASPECTS OF MAINTENANCE	No change.

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
MA-1.1	Define the security aspects of the maintenance strategy.	See Discussion.
MA-1.2	Identify the system constraints resulting from the security aspects of maintenance and logistics to be incorporated into the system requirements, architecture, and design.	No change.
MA-1.3	Identify trades such that the security aspects of system maintenance and logistics result in a solution that is trustworthy, secure, affordable, operable, supportable, and sustainable.	No change.
MA-1.4	Identify, plan for, and obtain enabling systems or services to support the security aspects of system maintenance and logistics.	No change.
MA-2	PERFORM THE SECURITY ASPECTS OF MAINTENANCE	No change.
MA-2.1	Review incident and problem reports to identify security relevance and associated maintenance needs.	No change.
MA-2.2	Record the security aspects of maintenance incidents and problems and track their resolution.	No change.
MA-2.3	Implement the procedures for the correction of random faults or scheduled replacement of system elements to ensure the ability to deliver system security functions and services.	No change.
MA-2.4	Implement action to restore the system to secure operational status when a random fault causes a system failure.	No change.
MA-2.5	Perform preventive maintenance by replacing or servicing system elements prior to failure with security-related impact.	No change.
MA-2.6	Perform failure identification actions when security noncompliance has occurred in the system.	No change.
MA-2.7	Identify when security-relevant adaptive or perfective maintenance is required.	No change.
MA-3	PERFORM THE SECURITY ASPECTS OF LOGISTICS SUPPORT	No change.
MA-3.1	Perform the security aspects of acquisition logistics.	No change.
MA-3.2	Perform the security aspects of operational logistics.	No change.
MA-3.3	Implement any secure packaging, handling, storage, and transportation needed during the life cycle of the system.	No change.
MA-3.4	Confirm that security aspects incorporated into logistics actions satisfy the required protection levels so that system elements are securely stored and able to meet repair rates and planned schedules.	No change.

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
MA-3.5	Confirm that the security aspects of logistics actions include security supportability requirements that are planned, resourced, and implemented.	No change.
MA-4	MANAGE RESULTS OF THE SECURITY ASPECTS OF MAINTENANCE AND LOGISTICS	No change.
MA-4.1	Record the security aspects of maintenance and logistics results and any security anomalies encountered.	No change.
MA-4.2	Record operational security incidents and security problems and track their resolution.	No change.
MA-4.3	Identify and record the security-related trends of incidents, problems, and maintenance and logistics actions.	No change.
MA-4.4	Maintain traceability of system elements and the security aspects of maintenance actions and logistics actions performed.	No change.
MA-4.5	Provide security-relevant configuration items from system maintenance to baselines.	No change.
MA-4.6	Monitor customer satisfaction with the security aspects of system	No change.

3.14 DISPOSAL

Cyber Resiliency Engineering Purpose

When considering cyber resiliency as part of the *Disposal* process, systems security engineering analyzes whether and how removing system elements, or the entire system-of-interest, can result in decreased cyber resiliency. Removal of a system element can reduce the extent to which some cyber resiliency techniques are used (e.g., Diversity, Redundancy, Segmentation) and can also reduce the effectiveness of some cyber resiliency techniques (e.g., Analytic Monitoring, Dynamic Representation). The disposal strategy should address the resulting risks. The relevance of cyber resiliency design principles to the remaining systems is determined, and the disposal strategy ensures that relevant design principles continue to be applied.

Cyber Resiliency Engineering Outcomes

- The risk to or the reduction in cyber resiliency of other systems, missions, business functions, or the organization due to removing system elements, or withdrawing the system-of-interest from operations, if any, is understood and accepted by stakeholders.

Cyber Resiliency Considerations

DS-1.1 Develop the security **and cyber resiliency** aspects of the disposal strategy.

Discussion: The disposal strategy for the system identifies and provides steps to manage the potential consequences of the permanent termination of system functions and delivery on the ability of other systems to achieve or maintain stated cyber resiliency objectives. Similarly, the system disposal strategy addresses the potential consequences of transforming the system and its environment into an acceptable state on the

ability of other systems to achieve or maintain stated cyber resiliency objectives. Consideration should also be given to hazards or threats resulting from residue left behind from the disposal of the system or system element. For example, materials related to the operational context of a predecessor system may still be relevant to a successor system or system element and therefore may have value to an adversary.

Table 18 lists the cyber resiliency considerations for the *Disposal* process.

TABLE 18: CYBER RESILIENCY CONSIDERATIONS FOR DISPOSAL

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
DS-1	PREPARE FOR THE SECURITY ASPECTS OF DISPOSAL	Change "security aspects" to "security and cyber resiliency aspects."
DS-1.1	Develop the security aspects of the disposal strategy.	Change "security aspects" to "security and cyber resiliency aspects." See Discussion.
DS-1.2	Identify the system constraints resulting from the security aspects of disposal to be incorporated into the system requirements, architecture, and design.	Change "security aspects" to "security and cyber resiliency aspects."
DS-1.3	Identify, plan for, and obtain the enabling systems or services to support the secure disposal of the system.	No change.
DS-1.4	Specify secure storage criteria for the system if it is to be stored.	No change.
DS-1.5	Identify and preclude terminated personnel or disposed system elements and materials from being returned to service.	No change.
DS-2	PERFORM THE SECURITY ASPECTS OF DISPOSAL	Change "security aspects" to "security and cyber resiliency aspects."
DS-2.1	Deactivate the system or system element to prepare it for secure removal from operation.	No change.
DS-2.2	Securely remove the system or system element from use for appropriate secure disposition and action.	No change.
DS-2.3	Securely withdraw impacted operating staff from the system and record relevant secure operation knowledge.	No change.
DS-2.4	Disassemble the system or system element into manageable components and ensure that appropriate protections are in place for those components during removal for reuse, recycling, reconditioning, overhaul, archiving, or destruction.	No change.
DS-2.5	Sanitize system elements and life cycle artifacts in a manner appropriate to the disposition action.	No change.
DS-2.6	Manage system elements and their parts that are not intended for reuse to prevent them from re-entering the supply chain.	No change.
DS-3	FINALIZE THE SECURITY ASPECTS OF DISPOSAL	Change "security aspects" to "security and cyber resiliency aspects."
DS-3.1	Confirm that no unresolved security factors exist following disposal of the system.	No change.

IDENTIFIER	ACTIVITY OR TASK	CYBER RESILIENCY CONSIDERATIONS
DS-3.2	Return the environment to its original state or to a secure state specified by agreement.	No change.
DS-3.3	Archive and protect information generated during the life cycle of the system.	No change.

ENGINEERING FOR CYBER RESILIENCY INVOLVES JUDGMENT

THERE IS NO SINGLE SOLUTION

As with the fundamental constructs (e.g., goals, objectives, techniques, approaches, and design principles) and practices (e.g., analysis, modeling, scoring, measuring, trades, and visualizing effects) of any specialty engineering discipline, the constructs and practices for cyber resiliency described in this publication should be applied selectively. Stakeholders will prioritize goals and objectives; while different stakeholders may prioritize these differently, the overall priorities for one system-of-interest may be quite different from those for another system-of-interest. The applicability of techniques, approaches, and design principles depends on the type of the system-of-interest (e.g., cyber-physical system vs. enterprise information technology), as well as on the types of engineering decisions which can be made (e.g., design decisions restricted to a specific architectural layer, decisions restricted by the life cycle stage—design decisions vs. decisions to implement compensating procedural controls).

Therefore, the integration of engineering practices for cyber resiliency into systems engineering processes calls upon systems engineers to exercise judgment about the relative priorities and applicability of cyber resiliency constructs, and the relative effectiveness of alternative cyber resiliency solutions—ultimately, to deliver a trustworthy system.

APPENDIX A

REFERENCES

KEY REFERENCES RELATED TO SYSTEMS SECURITY ENGINEERING AND CYBER RESILIENCY[35]

LEGISLATION, POLICIES, DIRECTIVES, INSTRUCTIONS	
[FISMA]	Federal Information Security Modernization Act of 2014, (P.L. 113-283, Title II), December 2014. https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[CNSSI 4009]	Committee on National Security Systems (CNSS) Instruction No. 4009, *Committee on National Security Systems (CNSS) Glossary*, April 2015. https://www.cnss.gov
[DOD 8140.01]	Department of Defense (DoD) Directive 8140.01, *Cyberspace Workforce Management*, August 2015. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001_2015_dodd.pdf
[PPD-8]	Presidential Policy Directive (PPD) 8, *National Preparedness*, March 2011. https://www.dhs.gov/xlibrary/assets/presidential-policy-directive-8-national-preparedness.pdf
[PPD-21]	Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Resilience*, February 2013. https://www.dhs.gov/sites/default/files/publications/PPD-21-Critical-Infrastructure-and-Resilience-508.pdf
STANDARDS AND GUIDELINES	
[FIPS 199]	National Institute of Standards and Technology, Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. https://doi.org/10.6028/NIST.FIPS.199
[ISO/IEC/IEEE 15288]	International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 15288:2015, *Systems and software engineering — Systems life cycle processes*, May 2015.
[NIST 800-30]	National Institute of Standards and Technology Special Publication 800-30 Revision 1, *Guide for Conducting Risk Assessments*, September 2012. https://doi.org/10.6028/NIST.SP.800-30r1

[35] References in this section without specific publication dates or revision numbers are assumed to refer to the most recent updates to those publications.

[NIST 800-34] National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010. https://doi.org/10.6028/NIST.SP.800-34r1

[NIST 800-37] National Institute of Standards and Technology Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010. https://doi.org/10.6028/NIST.SP.800-37r1

[NIST 800-39] National Institute of Standards and Technology Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011. https://doi.org/10.6028/NIST.SP.800-39

[NIST 800-53] National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013. https://doi.org/10.6028/NIST.SP.800-53r4

[NIST 800-53 R5] National Institute of Standards and Technology Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, Initial Public Draft, August 2017. https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

[NIST 800-82] National Institute of Standards and Technology Special Publication 800-82, Revision 2, *Guide to Industrial Control Systems (ICS) Security*, May 2015. https://doi.org/10.6028/NIST.SP.800-82r2

[NIST 800-95] National Institute of Standards and Technology Special Publication 800-95, *Guide to Secure Web Services*, August 2007. http://doi.org/10.6028/NIST.SP.800-95

[NIST 800-125] National Institute of Standards and Technology Special Publication 800-125, *Guide to Security for Full Virtualization Technologies*, January 2011. https://doi.org/10.6028/NIST.SP.800-125

[NIST 800-160 Vol. 1] National Institute of Standards and Technology Special Publication 800-160, Volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, November 2016. https://doi.org/10.6028/NIST.SP.800-160

[NIST 1190] National Institute of Standards and Technology Special Publication 1190, *Community Resilience Planning Guide for Buildings and Infrastructure Systems, Volume I*, May 2016. http://dx.doi.org/10.6028/NIST.SP.1190v1

[NIST 1500-201] National Institute of Standards and Technology Special Publication 1500-201, *Framework for Cyber-Physical Systems: Volume 1, Overview*, June 2017. https://www.nist.gov/publications/framework-cyber-physical-systems-volume-1-overview

[MIL-STD-882E] MIL-STD-882E, *Standard Practice – System Safety, Department of Defense (DoD)*, May 2012.

OTHER PUBLICATIONS

[Avizienis04] A. Avižienis, J. C. Laprie and B. Randell, "Dependability and Its Threats: A Taxonomy," in *Building the Information Society. IFIP International Federation for Information Processing*, Vol. 156, Boston, MA, Springer, 2004, pp. 91-120.

[Bodeau11] D. Bodeau and R. Graubart, "Cyber Resiliency Engineering Framework, Version 1.0," September 2011.

[Bodeau15] D. Bodeau, R. Graubart, W. Heinbockel and E. Laderman, "Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques, (MTR140499R1, PR 15-1334)," May 2015. http://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf

[Bodeau16] D. Bodeau and R. Graubart, "Cyber Prep 2.0: Motivating Organizational Cyber Strategies in Terms of Preparedness (MTR 150264, PR 16-0939)," The MITRE Corporation, Bedford, MA, 2016.

[Bodeau17] D. Bodeau and R. Graubart, "Cyber Resiliency Design Principles: Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines (MTR 170001, PR 17-0103)," The MITRE Corporation, Bedford, MA, 2017.

[Brtis16] J. Brtis, "How to Think about Resilience in a DoD Context (MTR 160138, PR 16-2051)", The MITRE Corporation, Colorado Springs, CO, 2016.

[Clemen13] R. T. Clemen and T. Reilley, *Making Hard Decisions with the Decision Tools Suite, 3rd Edition*, Cengage Learning, 2013.

[DHS10] Department of Homeland Security, *DHS Risk Lexicon*, September 2010.

[DoD15] DoD, "Department of Defense Cybersecurity Test and Evaluation Guidebook, Version 1.0," July 2015.

[DSB13] Defense Science Board (DSB), "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," January 2013. http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

[Folk15] C. Folk, D. C. Hurley, W. K. Kaplow and J. F. Payne, "The Security Implications of the Internet of Things," AFCEA International Cyber Committee, February 2015. http://www.afcea.org/site/sites/default/files/files/AFC_WhitePaper_Revised_Out.pdf

[Heckman15] K. E. Heckman, F. J. Stech, R. K. Thomas, B. Schmoder and A. W. Tsow, *Cyber Denial, Deception and Counter Deception: A Framework for Supporting Active Cyber Defense* (Advances in Information Security 63), Switzerland: Springer, 2015.

[Höller15] A. Höller, T. Rauter, J. Iber and C. Kreiner, "Towards Dynamic Software Diversity for Resilient Redundant Embedded Systems (Lecture Notes in Computer Science 9274)," in *Proceedings of Software Engineering for Resilient Systems: 7th International Workshop, SERENE 2015*, Switzerland, Springer, 2015, pp. 16-30.

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

[IEEE17] IEEE, "Enterprise IT Body of Knowledge - Glossary," Enterprise IT Body of Knowledge, December 2017. http://eitbokwiki.org/Glossary#eit

[INCOSE11] International Council for Systems Engineering, "Resilient Systems Working Group Charter," November 2011.

[INCOSE14] International Council on Systems Engineering, *System Engineering Handbook—A Guide for System Engineering Life Cycle Processes and Activities*, TP-2003-002-04, 4th Edition, July 2015.

[ISACA] ISACA Glossary of Terms https://www.isaca.org/pages/glossary.aspx

[Jackson07] S. Jackson, "A Multidisciplinary Framework for Resilience to Disasters and Disruptions," Journal of Integrated Design and Process Science, Vol. 11, No. 2, pp. 91-108, 2007.

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

[Jajodia11] S. Jajodia, A. K. Ghosh, V. Swarup, C. Wang and X. S. Wang (editors), *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats* (Advances in Information Security, Vol. 54), Springer, 2011.

[Jajodia12] S. Jajodia, A. K. Ghosh, V. S. Subrahmanian, V. Swarup, C. Wang, and X. S. Wang (editors), *Moving Target Defense II: Application of Game Theory and Adversarial Modeling* (Advances in Information Security), New York: Springer, 2012.

[King12] S. King, "National and Defense S&T Strategies & Initiatives," 25-26 July 2012.

[Madni07] A. M. Madni, *Designing for Resilience*, ISTI Lecture Notes on Advanced Topics in Systems Engineering 2007.

[Madni09] A. M. Madni and S. Jackson. "Towards a Conceptual Framework for Resilience Engineering," IEEE Systems Journal, Vol. 3, No. 2. June 2009.

[Maier98] M. Maier, *Architecting Principles for Systems-of-Systems*, The Aerospace Corporation, 1998.

[MITRE07] *Common Attack Pattern Enumeration and Classification (CAPEC)*, The MITRE Corporation, 2007. https://capec.mitre.org/index.html

[MITRE16] *Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)*, The MITRE Corporation, 2016. https://attack.mitre.org/wiki/Main_Page

[Musman18] S. Musman et al. "A Measurable Definition of Resilience using "Mission Risk" as a Metric," *The Cyber Resilience of Systems and Networks*, Springer Lecture Notes [TBD], 2018.

[Neumann04] P. Neumann, *Principled Assuredly Trustworthy Composable Architectures*, CDRL A001 Final Report, SRI International, Menlo Park, CA, December 28, 2004.

[NIAC10] National Infrastructure Advisory Council (NIAC), *A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations by the Council*, October 2010.

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

[NISTIR 8062] National Institute of Standards and Technology Internal Report 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, January 2017.

[NIST CSF] National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 2014. https://www.nist.gov/cyberframework

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

[Okhravi13] H. Okhravi, M. A. Rabe, T. J. Mayberry, W. G. Leonard, T. R. Hobson, D. Bigelow and W. W. Streilein, "Survey of Cyber Moving Targets," ESC-EN-HA-TR-2012-109, Technical Report 1166, September 2013.

[Ricci14] N. Ricci, D. H. Rhodes and A. M. Ross, "Evolvability-Related Options in Military Systems of Systems," in *Conference on Systems Engineering Research (CSER 2014)*, Redondo Beach, CA, 2014.

[Richards08] M. G. Richards, A. M. Ross, D. E. Hastings and D. H. Rhodes, "Empirical Validation of Design Principles for Survivable System Architecture," in *Proceedings of the 2nd Annual IEEE Systems Conference*, Montreal, Quebec, Canada, 2008.

[Richards09] M. G. Richards, D. E. Hastings, D. H. Rhodes, A. M. Ross and A. L. Weigel, "Design for Survivability: Concept Generation and Evaluation in Dynamic Tradespace Exploration," in *Second International Symposium on Engineering Systems*, Cambridge, MA, 2009.

[SEBok] *Guide to the Systems Engineering Body of Knowledge (SEBoK)*, International Council on Systems Engineering (INCOSE), the Systems Engineering Research Center (SERC), and the IEEE Computer Society. http://www.sebokwiki.org/wiki/Guide_to_the_Systems_Engineering_Body_of_Knowledge_(SEBoK)

[Sheard08] S. Sheard, "A Framework for System Resilience Discussions," in *INCOSE International Symposium 18*, Utrecht, the Netherlands, Wiley, 2008, pp. 1243–1257.

[Shetty16] S. Shetty, X. Yuchi and M. Song, *Moving Target Defense for Distributed Systems*, Switzerland: Springer, 2016.

[Sterbenz06] J. Sterbenz and D. Hutchinson, *ResilieNets: Multilevel Resilient and Survivable Networking Initiative*, August 2006.

[Sterbenz10] J. P. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," March 2010. http://www.ittc.ku.edu/resilinets/papers/Sterbenz-Hutchison-Cetinkaya-Jabbar-Rohrer-Scholler-Smith-2010.pdf

[Sterbenz14] J. P. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller and P. Smith, "Redundancy, diversity, and connectivity to achieve multilevel network resilience, survivability, and disruption tolerance," *Journal of Telecommunications Systems*, Vol. 56, No. 1, pp. 17-31, 2014.

[Strom17] B. Strom, et.al., "Finding Cyber Threats with ATT&CK™-Based Analytics," The MITRE Corporation, June 2017. https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats%20with%20att%26ck-based-analytics.pdf

[Temin10] A. Temin and S. Musman, "A Language for Capturing Cyber Impact Effects, MTR 100344, PR 10-3793," The MITRE Corporation, Bedford, MA, 2010.

[Zimmerman14] C. Zimmerman, "Ten Strategies of a World-Class Cybersecurity Operations Center," October 2014. http://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf

[Ware70] W. Ware, *Security Controls for Computer Systems*, Report of the Defense Science Board Task Force on Computer Security, February 1970.

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

This appendix provides definitions for terminology used within Special Publication 800-160, Volume 2. Definitions that do not include a source reference can be attributed to content in this publication or to commonly understood terminology.

active entity [NIST 800-53]	A user or a process acting on behalf of a user. Also referred to as a subject.
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 persistent threat [NIST 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.
adversity	Adverse conditions, stresses, attacks, or compromises. *Note 1:* The definition of adversity is consistent with the use of the term in [NIST 800-160, Vol. 1] 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 [NIST 800-160, Vol. 1]	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.
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.
criticality [NIST 800-160, Vol. 1]	An attribute assigned to an asset that reflects its relative importance or necessity in achieving or contributing to the achievement of stated goals.
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 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, capabilities) may be used in some modeling and analytic practices.
cyber resiliency control	A security or privacy control as defined in NIST SP 800-53 which requires the use of one or more cyber resiliency techniques or implementation 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 techniques, approaches, and solutions when making architectural or design decisions.
cyber resiliency engineering practice	A method, process, modeling technique, or analytic technique used to identify and analyze cyber resiliency solutions.
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 solution	A combination of technologies, architectural decisions, systems engineering processes, and operational processes, procedures, or practices which 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 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.
cyberspace [CNSSI 4009, HSPD-23]	The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.
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/IEC/IEEE 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 [NIST 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.
information resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
information system [44 U.S.C., Sec. 3502]	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.

other system [ISO/IEC/IEEE 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 [NIST 800-160, Vol. 1]	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.
reliability [IEEE90]	The ability of a system or component to function under stated conditions for a specified period of time.
resilience [OMB Circular 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.
[INCOSE]	The ability to maintain required capability in the face of adversity."
resilient otherwise [NIST 800-160, Vol. 1]	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 No. 4009, OMB Circular 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-adaptive access control [NIST 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 [NIST 800-30]	A characteristic used in a risk model as an input to determining the level of risk in a risk assessment.

risk framing [NIST 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 model [NIST 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.
safety [NIST 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 [NIST 800-160, Vol. 1]	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 [NIST 800-160, Vol. 1]	Freedom from those conditions that can cause loss of assets with unacceptable consequences.
security control [NIST 800-160, Vol. 1]	A mechanism designed to address needs as specified by a set of security requirements.
security controls [OMB Circular 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. *Note:* Security criteria related to a supplier's ability may require specific human resources, capabilities, methods, technologies, techniques, or tools to deliver an acceptable product or service with the desired level of assurance and trustworthiness. Security criteria related to a system's ability to meet security requirements may be expressed in quantitative terms (i.e., metrics and threshold values), in qualitative terms (including threshold boundaries), or in terms of identified forms of evidence.
security function [NIST 800-160, Vol. 1]	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 [NIST 800-160, Vol. 1]	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 [NIST 800-160, Vol. 1]	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/IEC/IEEE 15288, NIST 800-160, Vol. 1]	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 [NIST 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/IEC/IEEE 15288, NIST 800-160, Vol. 1]	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 [NIST 800-160, Vol. 1]	A system whose life cycle is under consideration in the context of [ISO/IEC/IEEE 15288]. *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 [NIST 800-160, Vol. 1, 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.
technique	See *cyber resiliency technique*.
threat event [NIST 800-30]	An event or situation that has the potential for causing undesirable consequences or impact.
threat scenario [NIST 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 No. 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 [NIST 800-160, Vol. 1]	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.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

ABAC	Attribute-Based Access Control
ACR	Adversary-driven Cyber Resiliency (Analysis)
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
ASIC	Application-Specific Integrated Circuit
ASLR	Address Space Layout Randomization
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge
BIA	Business Impact Analysis
C3	Command, Control, and Communications
CAN	Controller Area Network
CAPEC	Common Attack Pattern Enumeration and Classification
CDM	Continuous Diagnostics and Monitoring
CDS	Cross-Domain Solution
CE	Control Enhancement
CERT	Computer Emergency Response team
CIS	Critical Infrastructure System
CJA	Crown Jewels Analysis Cyber
CMIA	Cyber Mission Impact Analysis
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COOP	Continuity of Operations
COTS	Commercial Off-The-Shelf
CPS	Cyber-Physical System or Systems
CRR	Cyber Resilience Review
DHS	Department of Homeland Security
DMZ	De-Militarized Zone
DNS	Domain Name Service
DoD	Department of Defense
DoDI	Department of Defense Instruction
DSB	Defense Science Board

DSP	Digital Signal Processor
EIT	Enterprise Information Technology
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
FOSS	Free and Open Source Software
GPS	Global Positioning System
HACS	Highly Adaptive Cybersecurity Services
HDL	Hardware Description Language
IdAM	Identity and Access Management
IACD	Integrated Adaptive Cyber Defense
ICS	Industrial Control System
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
MIA	Mission Impact Analysis
MIL-STD	Military Standard
M&S	Modeling and Simulation Modeling
MBSE	Model-Based Systems Engineering
MOE	Measures of Effectiveness
MOP	Measures of Performance
MTD	Moving Target Defense
NASA	National Aeronautics and Space Administration
NIAC	National Infrastructure Advisory Council
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report

OMB	Office of Management and Budget
OPSEC	Operations Security
OS	Operating System
OT	Operational Technology
PII	Personally Identifiable Information
PPD	Presidential Policy Directive
PPP	Program Protection Plan
RAdAC	Risk-Adaptive Access Control
RAID	Redundant Array of Independent Disks
RBAC	Role-Based Access Control
RMM	Resilience Management Model
RSWG	(INCOSE) Resilient Systems Working Group
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SEI	Software Engineering Institute
SLA	Service-Level Agreement
SOC	Security Operations Center
SP	Special Publication
SSE	Systems Security Engineering
TTPs	Tactics, Techniques, and Procedures
VOIP	Voice over Internet Protocol
VPN	Virtual Private Network

APPENDIX D

CYBER RESILIENCY TECHNIQUES

DESCRIPTION AND PURPOSE OF CYBER RESILIENCY TECHNQUES

This appendix 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 to include specific mapping tables for the constructs is provided in Appendix H. Table D-1 lists each cyber resiliency technique and its purpose. Table D-2 identifies potential interactions (e.g., synergies and conflicts) between cyber resiliency techniques.

TABLE D-1: CYBER RESILIENCY TECHNIQUES

TECHNIQUE	PURPOSE
Adaptive Response Implement agile cyber courses of action to manage risks.	Optimize the ability to respond in a timely and appropriate manner to adverse conditions, stresses, or attacks, or to indicators of these, thus maximizing the ability to maintain mission or business operations, limit consequences, and avoid destabilization.
Analytic Monitoring 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, and identify potential or actual damage. Provide data needed for situational awareness.
Coordinated Protection 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 Mislead, confuse, hide critical assets from, or expose covertly tainted assets to, the adversary.	Mislead or confuse the adversary, or hide critical assets from the adversary, making the adversary uncertain 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 Use heterogeneity to minimize common mode failures, particularly attacks exploiting common vulnerabilities.	Limit the possibility of loss of critical functions due to 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 Distribute and dynamically relocate functionality or system resources.	Increase the ability to rapidly recover from non-adversarial events (e.g., fires, floods). Impede an adversary's ability to locate, eliminate, or corrupt mission or business assets, and cause the adversary to spend more time and effort to find the organization's critical assets, thereby increasing the probability of the adversary revealing its actions and tradecraft prematurely.

TECHNIQUE	PURPOSE
Dynamic Representation Construct and maintain current representations of the posture of missions or business functions considering cyber events and cyber courses of action.	Support situational awareness. Enhance understanding of dependencies among cyber and non-cyber resources. Reveal patterns or trends in adversary behavior.
Non-Persistence 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.
Privilege Restriction Restrict privileges based on 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 Align system resources with core aspects of organizational missions or business functions.	Minimize the connections between mission-critical and noncritical services, thus reducing the likelihood that a failure of noncritical 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.
Redundancy Provide multiple protected instances of critical resources.	Reduce the consequences of 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 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 easily be propagated.
Substantiated Integrity Ascertain whether critical system elements have been corrupted.	Facilitate 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 Make changes randomly or unpredictably.	Increase an adversary's uncertainty regarding the system protections which they may encounter, thus making it more difficult for them to ascertain the appropriate course of action.
Shortcut to Section 2.2.3 Shortcut to Table H-2 Shortcut to Table H-4 Shortcut to Section F.2 Shortcut to Appendix J	

TABLE D-2: POTENTIAL INTERACTIONS BETWEEN CYBER RESILIENCY TECHNIQUES

Technique / Enabler B Technique A	Adaptive Response	Analytic Monitoring	Coordinated Protection	Deception	Diversity	Dynamic Positioning	Dynamic Representation	Non-Persistence	Privilege Restriction	Realignment	Redundancy	Segmentation	Substantiated Integrity	Unpredictability
Adaptive Response	-	D	S		U	U, S	U	U, S	U, S		U	U, S	U	U
Analytic Monitoring	S	-	D	U, C	U	U	S						U, S	
Coordinated Protection	U	S	-		U				U, S	U		U		
Deception		U, C		-		U						U	S	U
Diversity	S	C, S	C, S		-	S	C		U	U	S		U	S
Dynamic Positioning	U, S	C, S		S	U	-		U			U			U, S
Dynamic Representation	S	U					-			S			U	
Non-Persistence	U, S	C				S	C	-					U	S
Privilege Restriction	S		U						-	S			U	
Realignment	C		C, S		C, S		U		S	-	C			
Redundancy	S				U	S					-		U	
Segmentation	U, S	C	S	S								-		U
Substantiated Integrity	S	S, U		U	S		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.

APPENDIX E

IMPLEMENTATION APPROACHES

REPRESENTATIVE APPROACHES TO IMPLEMENTING CYBER RESILIENCY TECHNIQUES

This appendix identifies representative cyber resiliency *approaches* to implementing cyber resiliency techniques. An approach is a subset of the technologies and processes included in a cyber resiliency technique, defined by how the capabilities are implemented or how the intended consequences are achieved. Table E-1 lists each cyber resiliency technique, the representative approaches that can be employed to implement the technique, and representative examples. Where possible, examples are drawn from the discussions associated with the controls and control enhancements in [NIST 800-53], even when these controls or enhancements do not directly support cyber resiliency as described in Appendix G. However, [NIST 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, 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.

TABLE E-1: CYBER RESILIENCY APPROACHES

TECHNIQUES	APPROACHES	EXAMPLES
Adaptive Response Implement nimble cyber courses of action to manage risks.	**Dynamic Reconfiguration** Make changes to individual systems, system elements, components, or sets of cyber resources to change functionality or behavior without interrupting service.	• Dynamically change router rules, access control lists, intrusion detection and prevention system parameters, and filter rules for firewalls and gateways.
	Dynamic Resource Allocation Change the allocation of 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. • Pre-empt communications.
	Adaptive Management Change how mechanisms are used based on changes in the operational environment as well as changes in the threat environment.	• Disable access dynamically. • Implement adaptive authentication. • Provide for automatic disabling of the system. • Provide dynamic deployment of new or replacement resources or capabilities.
Shortcut to Table H-2	Shortcut to Table H-5	Shortcut to Appendix J
Analytic Monitoring Monitor and analyze a wide range of properties and behaviors on an ongoing basis and in a coordinated way.	**Monitoring and Damage Assessment** Monitor and analyze behavior and characteristics of components and resources to look for indicators of	• Employ Continuous Diagnostics and Mitigation (CDM) or other vulnerability scanning tools. • Deploy Intrusion Detection Systems (IDSs) and other monitoring tools.

TECHNIQUES	APPROACHES	EXAMPLES
	adversary activity, and to detect and assess damage from adversity.	• Use Insider Threat monitoring tools. • Perform telemetry analysis. • Detect malware beaconing. • Monitor open source information for indicators of disclosure or compromise.
	Sensor Fusion and Analysis Fuse and analyze monitoring data and analysis results from different components, together with externally provided threat intelligence.	• Enable organization-wide situational awareness. • Implement cross-organizational auditing. • Correlate data from different tools. • Fuse data from physical access control systems and information systems.
	Malware and Forensic Analysis Analyze malware and other artifacts left behind by adverse events.	• Deploy an integrated team of forensic and malware analysts, developers, and operations personnel. • Use reverse engineering and other malware analysis tools.
Shortcut to Table H-2	Shortcut to Table H-5	Shortcut to Appendix J
Coordinated Protection Ensure that protection mechanisms operate in a coordinated and effective manner.	**Calibrated Defense-in-Depth** Provide complementary protective mechanisms at different architectural layers or in different locations, calibrating the strength and number of mechanisms to resource value.	• 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 Determine whether and how protections can be applied in a coordinated, consistent way that minimizes interference, potential cascading failures, or coverage gaps.	• Employ unified IdAM administration tools. • Analyze mission/business process flows and threads. • Employ privilege analysis tools to support an ongoing review of whether user privileges are assigned consistently. • Interpret attributes consistently. • Coordinate the planning, training, and testing of incident response, contingency planning, etc. • Design for facilitating coordination and mutual support among safeguards.
	Orchestration Coordinate the ongoing behavior of mechanisms and processes at	• Coordinate incident handling with mission/business process continuity

TECHNIQUES	APPROACHES	EXAMPLES
	different layers, in different locations, or implemented for different aspects of trustworthiness to avoid causing cascading failures, interference, or coverage gaps.	of operations and organizational processes. • Conduct coverage planning and management for sensors. • Use cyber playbooks.
	Self-Challenge Affect mission/business processes or system elements adversely in a controlled manner, to validate the effectiveness of protections and to enable proactive response and improvement.	• Conduct role-based training exercises. • Conduct penetration testing and Red Team exercises. • Test automated incident response. • Employ fault injection. • Conduct tabletop exercises.
Shortcut to Table H-2	Shortcut to Table H-5	Shortcut to Appendix J
Deception Mislead, confuse, hide critical assets from, or expose covertly tainted assets to the adversary.	**Obfuscation** Hide, transform, or otherwise obfuscate information from the adversary.	• Encrypt data at rest. • Encrypt transmitted data (e.g., using VPNs). • Encrypt authenticators. • Conceal or randomize communications patterns. • Conceal the presence of system components on an internal network. • Mask, encrypt, hash, or replace identifiers. • Obfuscate traffic via onion routing. • Perform encrypted processing.
	Disinformation Provide deliberately misleading information to adversaries.	• Post questions to a public forum based on false information about the system. • Create false credentials.
	Misdirection Maintain deception resources or environments and direct adversary activities there.	• Establish and maintain honeypots or decoys. • Maintain a full-blown deception environment.
	Tainting Embed covert capabilities in resources.	• Use beacon traps. • Employ internal network table cache poisoning (e.g., DNS, ARP). • Include false entries or steganographic data in files to enable them to be found via open source analysis.
Shortcut to Table H-2	Shortcut to Table H-5	Shortcut to Appendix J
Diversity Use heterogeneity to minimize common mode failures, particularly attacks exploiting common vulnerabilities.	**Architectural Diversity** Use multiple sets of technical standards, different technologies, and different architectural patterns.	• Use a different OS than the one being audited to store audit data. • Deploy diverse operating systems. • Support multiple protocol standards.
	Design Diversity	• Employ N-version programming.

TECHNIQUES	APPROACHES	EXAMPLES
	Use different designs to meet the same requirements or provide equivalent functionality.	• Employ mixed-signal design diversity (using both analog and digital signals). • Employ mixed-level design diversity (using both hardware and software implementations).
	Synthetic Diversity Transform implementations of software to produce a variety of instances.	• Implement address space layout randomization. • Use randomizing compilers.
	Information Diversity Provide information from different sources or transform information in different ways.	• Apply different analog-to-digital conversion methods to non-digitally-obtained data. • Use multiple data sources.
	Path Diversity Provide multiple independent paths for command, control, and communications.	• Establish alternate telecommunications services (e.g., ground-based circuits, satellite communications). • Employ alternate communications protocols. • Use out-of-band channels.
	Supply Chain Diversity Use multiple independent supply chains for critical components.	• Use a diverse set of suppliers.
Shortcut to Table H-2	Shortcut to Table H-5	Shortcut to Appendix J
Dynamic Positioning Distribute and dynamically relocate functionality or system resources.	**Functional Relocation of Sensors** Relocate sensors, or reallocate responsibility for specific sensing tasks, to look for indicators of adverse events.	• Relocate (using virtualization) or reconfigure IDSs or IDS sensors.
	Functional Relocation of Cyber Resources Change the location of cyber resources that provide functionality or information, either by moving the assets or by transferring functional responsibility.	• 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 Securely move physical resources.	• 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 Fragment information and distribute it across multiple components.	• Implement fragmentation and partitioning for distributed databases.

TECHNIQUES	APPROACHES	EXAMPLES
	Distributed Functionality Distribute functionality (e.g., processing, storage, and communications) across multiple components.	• Distribute processing and storage across multiple components or physical locations.
Shortcut to Table H-2	Shortcut to Table H-5	Shortcut to Appendix J
Dynamic Representation Construct and maintain current representations of the posture of missions or business functions considering cyber events and cyber courses of action.	**Dynamic Mapping and Profiling** Maintain current information about resources, status of resources, and resource connectivity.	• Maintain real-time integrated situational awareness.
	Dynamic Threat Modeling Maintain current information about threat actors and potential, predicted, and observed adverse events.	• Track predicted or impending natural disasters. • Dynamically ingest incident and threat data. • Facilitate integrated situational awareness of threats.
	Mission Dependency and Status Visualization Maintain current information about the status of missions or business functions, dependencies on resources, and the status of those resources with respect to threats.	• Construct a broad (mission/business function-wide, organization-wide) perspective.
Shortcut to Table H-2	Shortcut to Table H-5	Shortcut to Appendix J
Non-Persistence Generate and retain resources as needed or for a limited time.	**Non-Persistent Information** Refresh information periodically, or generate information on demand, and delete it when no longer needed.	• Delete high-value mission information after it is processed. • Off-load audit records to off-line storage.
	Non-Persistent Services Refresh services periodically, or generate services on demand and terminate services when no longer needed.	• Employ time-based or inactivity-based session termination. • Re-image components. • Refresh services using virtualization.
	Non-Persistent Connectivity Establish connections on demand, and terminate connections when no longer needed.	• Implement software-defined networking. • Employ time-based or inactivity-based network disconnection.
Shortcut to Table H-2	Shortcut to Table H-5	Shortcut to Appendix J
Privilege Restriction Restrict privileges based on attributes of users and system elements as well as on environmental factors.	**Trust-Based Privilege Management** Define, assign, and maintain privileges associated with active entities, based on established trust criteria, consistent with principles of least privilege.	• Implement least privilege. • Employ time-based account restrictions.
	Attribute-Based Usage Restriction Define, assign, maintain, and apply usage restrictions on systems	• Employ Role-Based Access Control (RBAC).

TECHNIQUES	APPROACHES	EXAMPLES
	containing cyber resources based on the criticality of missions or business functions and other attributes (e.g., data sensitivity).	• Employ Attribute-Based Access Control (ABAC). • Restrict the use of maintenance tools.
	Dynamic Privileges Elevate or decrease privileges assigned to a user, process, or service based on transient or contextual factors.	• Implement time-based adjustment to privileges due to 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.
Shortcut to Table H-2	Shortcut to Table H-5	Shortcut to Appendix J
Realignment Align system resources with core aspects of organizational missions or business functions.	**Purposing** Ensure systems containing cyber resources are used consistent with critical mission or business function purposes.	• Use whitelisting to prevent installation of such unapproved applications as games or peer-to-peer music sharing. • Ensure that privileged accounts are not used for non-privileged functions.
	Offloading Offload supportive but non-essential functions to other systems or to an external provider that is better able to support the functions.	• Outsource non-essential services to a managed service provider. • Impose requirements on and perform oversight of external system services.
	Restriction Remove or disable unneeded functionality or connectivity, or add mechanisms to reduce the chance of vulnerability or failure.	• Configure the system to provide only essential capabilities. • Minimize non-security functionality.
	Replacement Replace low-assurance or poorly understood implementations with more trustworthy implementations.	• Remove or replace unsupported system components to reduce risk.
	Specialization Modify the design of, augment, or configure critical cyber resources uniquely for the mission or business function to improve trustworthiness.	• Re-implement or custom develop critical components. • Develop custom system elements covertly. • Define and apply customized configurations.
Shortcut to Table H-2	Shortcut to Table H-5	Shortcut to Appendix J
Redundancy	**Protected Backup and Restore** Back up information and software (including configuration data and	• Retain previous baseline configurations.

TECHNIQUES	APPROACHES	EXAMPLES
Provide multiple protected instances of critical resources.	virtualized resources) in a way that protects its confidentiality, integrity, and authenticity, and enable restoration in case of disruption or corruption.	• Maintain and protect system-level backup information (e.g., operating system, application software, system configuration data).
	Surplus Capacity Maintain extra capacity for information storage, processing, or communications.	• Maintain spare parts. • Address surplus capacity in service-level agreements with external systems.
	Replication Duplicate hardware, information, backups, or functionality in multiple locations and keep them synchronized.	• Provide alternate audit capability. • 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.
Shortcut to Table H-2	Shortcut to Table H-5	Shortcut to Appendix J
Segmentation Define and separate system elements based on criticality and trustworthiness.	**Predefined Segmentation** Define enclaves, segments, or other types of resource sets based on criticality and trustworthiness, so that they can be protected separately and, if necessary, isolated.	• Use virtualization to maintain separate processing domains based on user privileges. • Use cryptographic separation for maintenance. • Partition application from system functionality. • Isolate security functions from non-security functions. • Isolate security tools and capabilities using physical separation. • Isolate components based on mission or business function. • Separate subnets for connecting to different security domains. • Employ system partitioning. • Employ process isolation. • Implement sandboxes and other confined environments. • Implement memory protection.
	Dynamic Segmentation and Isolation Change the configuration of enclaves or protected segments, or isolate resources, while minimizing operational disruption.	• Implement dynamic isolation of components. • Implement software-defined networking and VPNs to define new enclaves.

TECHNIQUES	APPROACHES	EXAMPLES
Shortcut to Table H-2	Shortcut to Table H-5	Shortcut to Appendix J
Substantiated Integrity Ascertain whether critical system elements have been corrupted.	**Integrity Checks** Apply and validate checks of the integrity or quality of information, components, or services.	• Use tamper-evident seals and anti-tamper coatings. • Use automated tools for data quality checking. • Use non-modifiable executables. • Use polling techniques to identify potential damage. • Implement cryptographic hashes. • Employ information input validation. • Validate components as part of SCRM. • Employ integrity checking on external systems.
	Provenance Tracking Identify and track the provenance of data, software, or hardware elements.	• Employ component traceability as part of Supply Chain Risk Management (SCRM). • Employ provenance tracking as part of SCRM. • Implement anti-counterfeit protections. • Implement trusted path. • Implement code signing.
	Behavior Validation Validate the behavior of a system, service, or device against defined or emergent criteria (e.g., requirements, patterns of prior usage).	• Employ detonation chambers. • Implement function verification. • Verify boot process integrity. • Implement fault injection to observe potential anomalies in error handling.
Shortcut to Table H-2	Shortcut to Table H-5	Shortcut to Appendix J
Unpredictability Make changes randomly or unpredictably.	**Temporal Unpredictability** Change behavior or state at times that are determined randomly or by complex functions.	• Require re-authentication at random intervals. • Perform routine actions at different times of day.
	Contextual Unpredictability Change behavior or state in ways that are determined randomly or by complex functions.	• Rotate roles and responsibilities. • Implement random channel-hopping.
Shortcut to Table H-2	Shortcut to Table H-5	Shortcut to Appendix J

APPENDIX F

DESIGN PRINCIPLES

APPLYING STRATEGIC AND STRUCTURAL DESIGN PRINCIPLES

This appendix provides a description of *strategic* and *structural* cyber resiliency design principles, a key construct in the cyber resiliency engineering framework. It also describes relationships with 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 Appendix F of [NIST 800-160, Vol. 1] are identified.[36] As noted in Section 2.2.4, strategic design principles express the organization's risk management strategy and structural design principles support the strategic design principles.

F.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 F-1 describes five strategic cyber resiliency design principles and identifies the related design principles from other disciplines.[37] [38]

[36] Appendix F of [NIST 800-160, Vol. 1] defines security design principles in three broad categories: Security Architecture and Design, Security Capability and Intrinsic Behaviors, and Life Cycle Security. For a more detailed discussion of the relationships between security design principles and cyber resiliency techniques as well as cyber resiliency design principles, see [Bodeau17].

[37] Resilience Engineering design principles are described in the Systems Engineering Body of Knowledge [SEBoK] and [Jackson13]. The 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 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 which 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 which 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).

[38] 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 capability 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).

TABLE F-1: STRATEGIC CYBER RESILIENCY DESIGN PRINCIPLES

STRATEGIC DESIGN PRINCIPLES	KEY IDEAS	RELATED DESIGN PRINCIPLES FROM OTHER DISCIPLINES
Shortcut to Table F-2	Shortcut to Table H-3	Shortcut to Appendix F.2
Focus on common critical assets.	Limited organizational and programmatic resources need to be applied where they can provide the greatest benefit. This results in a strategy of focusing first on assets which are both critical and common, then on those which are either critical or common.	**Security:** Inverse Modification Threshold. **Resilience Engineering:** Physical Redundancy, Layered Defense, Loose Coupling. **Survivability:** Failure Mode Reduction, Fail-Safe, Evolution.
Support agility and architect for adaptability.	Not only does the threat landscape change as adversaries evolve, so do technologies and the ways in which individuals and organizations use them. Both agility and adaptability are integral to the risk management strategy, in response to the risk framing assumption that unforeseen changes will occur in the threat, technical, and operational environment through a system's life cycle.	**Security:** Secure Evolvability, Minimized Sharing, Reduced Complexity. **Resilience Engineering:** Reorganization, Human Backup, Inter-Node Interaction. **Survivability:** Mobility, Evolution.
Reduce attack surfaces.	A large attack surface is difficult to defend, requiring ongoing effort to monitor, analyze, and respond to anomalies. Reducing attack surfaces reduces ongoing protection scope costs and makes the adversary concentrate efforts on a small set of locations, resources, or environments that can be more effectively monitored and defended.	**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.	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.	**Security:** Trusted Components, Self-Reliant Trustworthiness, Trusted Communications Channels. *Incompatible with Security:* Hierarchical Protection. **Resilience Engineering:** Human Backup, Localized Capacity, Loose Coupling.
Expect adversaries to adapt.	Advanced cyber adversaries invest time, effort, and intelligence-gathering to improve existing and develop new TTPs. Adversaries adapt in response to opportunities offered by new technologies or uses of technology, as well as to the knowledge they gain about defender TTPs.	**Security:** Trusted Communications Channels. **Resilience Engineering:** Reorganization, Drift Correction. **Survivability:** Evolution.
Shortcut to Table F-2	Shortcut to Table H-3	Shortcut to Section F.2

Strategic design principles are driven by an organization's risk management strategy—in particular, by its risk framing. Risk framing includes such considerations as assumptions about the threat 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.[39] 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 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 F-2. Relationships between design principles and other cyber resiliency constructs are identified in Appendix H.

TABLE F-2: 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**: None. **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 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.

Sections F.1.1 through F.1.5 provide detailed descriptions of the five *strategic* cyber resiliency principles.

F.1.1 FOCUS ON COMMON CRITICAL ASSETS

A focus on critical assets (i.e., resources valued due to their importance to mission or business accomplishment) is central to contingency planning, continuity of operations planning, and operational resilience, as well as to safety analysis. Critical assets can be identified using a variety of mission-oriented analysis techniques, including for example: Mission Impact Analysis (MIA);

[39] See [NIST 800-39].

Business Impact Analysis (BIA);[40] Functional Dependency Network Analysis (FDNA); Crown Jewels Analysis (CJA); and Mission Thread Analysis. Failure Modes, Effects, and Criticality Analysis (FMECA) can in some instances, reflect a safety-oriented approach.

Assets that are common to multiple missions or business functions are potential high-value targets for adversaries either because those assets are critical or because their compromise increases the adversaries' options for lateral motion[41] or persistence. Once an asset is identified as critical or common, further analysis involves:

- 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, but 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 which could be used in further malicious cyber activities), and what would constitute an acceptable (e.g., safe, secure) failure mode. Again, properties which are critical to one mission may be non-essential to another, and a failure mode which 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, for example, disabling noncritical functionality, restoration 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 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 a high priority for the application of selected cyber resiliency techniques. It recognizes that risk mitigation resources are limited, and enables systems engineers to focus resources where they will have the greatest potential impact on risk mitigation.

F.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 system 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. 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.

[40] See [NIST 800-34].

[41] 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.

Adaptability is the property of an architecture, a design, and/or an implementation which 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; externalization of rules and configuration data; and 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). Thus, analyses need to consider Redundancy, Adaptive Response, and 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, as well as 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 technical environments.

F.1.3 REDUCE ATTACK SURFACES

The term *attack surface* refers to accessible areas where weaknesses or deficiencies in systems (including hardware, software, and firmware components) provide opportunities for adversaries to exploit vulnerabilities [NIST 800-53]. The attack surface is the system's 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]. While some uses of the term focus on externally exposed vulnerabilities, the assumption that an adversary will penetrate an organization's systems means that internal exposures (i.e., vulnerabilities which 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, a mission or an organization can be said to have an attack surface, which might include people and processes. 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 identification or discovery of attack surfaces a priority in design analyses,[42] 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 which 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.

As indicated in Table F-3, several alternative strategies for reducing an attack surface can be identified. These strategies are expressed by different controls in [NIST 800-53] and apply different cyber resiliency techniques. In Table F-3, the **bolding** in the discussion of the control indicates how the control supports the strategy. These strategies can be reflected by different

[42] For example, [NIST 800-53] control SA-11 (7), Developer Security Testing | Attack Surface Reviews, calls for analysis of design and implementation changes.

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 F-3 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 the exposure of the mission or organization to adversary reconnaissance. Other supply chain protections can reduce the exposure of key components to tampering.

TABLE F-3: STRATEGIES FOR REDUCING ATTACK SURFACES

STRATEGY	SECURITY CONTROL SUPPORTING STRATEGY	RELATED TECHNIQUES
Reduce the extent (area) of the attack surface.	Attack surface reduction includes, for example, **employing the concept of layered defenses; applying the principles of least privilege and least functionality; deprecating unsafe functions; applying secure software development practices including, for example, reducing the amount of code executing and reducing entry points available to unauthorized users; and eliminating application programming interfaces (APIs) that are vulnerable to cyber-attacks**. SA-15 (5) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION [NIST 800-53]	Coordinated Protection Privilege Restriction Realignment
Reduce the exposure (aperture or structural accessibility) of the attack surface.	Attack surface reduction includes, for example, **applying the principle of least privilege, employing layered defenses**, applying the principle of least functionality (i.e., restricting ports, protocols, functions, and services), deprecating unsafe functions, and eliminating application programming interfaces (APIs) that are vulnerable to cyber-attacks. SA-15 (6) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION [NIST 800-53]	Privilege Restriction Coordinated Protection
	Component isolation reduces the attack surface of organizational information systems. SC-7 (20) BOUNDARY PROTECTION | DYNAMIC ISOLATION / SEGREGATION [NIST 800-53]	Adaptive Response Segmentation/Isolation
Reduce the duration (temporal accessibility) of attack surface exposure.	Mitigate risk from advanced persistent threats by significantly reducing the targeting capability of adversaries (i.e., **window of opportunity** and available attack surface) to initiate and complete cyber-attacks. SI-14 NON-PERSISTENCE [NIST 800-53]	Non-Persistence

F.1.4 ASSUME COMPROMISED RESOURCES

Many 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. Note that 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 privacy policies, or the safety of the larger system or environment of which the resource is a part [NIST 1500-201, NIST16], or can use the resource in an attack on other systems.

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, as well as the speed and extent of malware propagation. An increasing number of modeling and simulation techniques support 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, data of indeterminate quality) and linking these systemic consequences to mission consequences (e.g., mission failure, safety failure) or organizational consequences (e.g., loss of trust or reputation).

F.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 which includes but goes beyond the common practice of searching for and seeking ways to remediate vulnerabilities (or classes of vulnerabilities); a system which 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 [MITRE16], 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., cyber-attack life cycle or cyber kill chain models, CAPEC [MITRE07] or ATT&CK [MITRE16] classes), as well as 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 wider range of TTPs to achieve the same objectives.

F.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 F-4, many of the structural

design principles are consistent with or leverage design principles for security and/or resilience.[43] 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. The next three design principles 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 F-4: STRUCTURAL CYBER RESILIENCY DESIGN PRINCIPLES

STRUCTURAL DESIGN PRINCIPLES	KEY IDEAS	RELATED DESIGN PRINCIPLES FROM OTHER DISCIPLINES
Shortcut to Table F-5	Shortcut to Table F-6	Shortcut to Table H-4 Shortcut to Appendix F.2
Limit the need for trust.	Limiting the number of system elements that need to be trusted reduces the level of effort needed for assurance, as well as for 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 compromises or disruptions across components or services.	**Security:** Trusted Components, Least Privilege, Predicate Permission. **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, removing single points of attack or failure. However, architectures	**Resilience Engineering:** Absorption, Repairability. **Survivability:** Heterogeneity.

[43] The relationship between strategic and structural cyber resiliency design principles is presented in Table F-5.

STRUCTURAL DESIGN PRINCIPLES	KEY IDEAS	RELATED DESIGN PRINCIPLES FROM OTHER DISCIPLINES
	and designs should take cost and manageability into consideration to avoid introducing new risks.	
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.
Shortcut to Table F-5	Shortcut to Table F-6 Shortcut to Table H-4	Shortcut to Appendix F.2
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 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, providing 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.
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.
Shortcut to Table F-5	Shortcut to Table F-6 Shortcut to Table H-4	Shortcut to Appendix F.2
Determine ongoing trustworthiness.	Periodic or ongoing verification and/or validation of the integrity or correctness of data or software can increase the effort needed by an adversary seeking to modify or fabricate data or functionality. Similarly, periodic or ongoing analysis of the behavior of individual users, system components, and services can increase suspicion, triggering responses such as	**Security:** Self-Reliant Trustworthiness, Continuous Protection, Secure Metadata Management, Self-Analysis, Accountability and Traceability. **Resilience Engineering:** Neutral State. **Survivability:** Fail-Safe.

STRUCTURAL DESIGN PRINCIPLES	KEY IDEAS	RELATED DESIGN PRINCIPLES FROM OTHER DISCIPLINES
	closer monitoring, more restrictive privileges, or quarantine.	
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.
Shortcut to Table F-5	Shortcut to Table F-6	Shortcut to Table H-4 Shortcut to Appendix F.2

The selection of structural design principles is driven by strategic design principles, as shown in Table F-5.

TABLE F-5: STRATEGIC DESIGN PRINCIPLES DRIVE 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.[44] This guidance affects the selection and application of cyber resiliency techniques. (See Table H-4 for the relationship between structural design principles and cyber resiliency techniques.) Table F-6 describes the application of structural design principles and the intended effects on risk.

TABLE F-6: STRUCTURAL DESIGN PRINCIPLES AND EFFECTS ON RISK

STRUCTURAL DESIGN PRINCIPLES	INTENDED EFFECTS ON RISK
Limit the need for trust.	Reduce likelihood of harm due to malice, error, or failure.
Control visibility and use.	Reduce likelihood of occurrence of adversarial events; reduce likelihood of harm due to malice, error, or failure.
Contain and exclude behaviors.	Reduce likelihood of occurrence of adversarial events; reduce likelihood of harm due to malice, error, or failure.
Layer defenses and partition resources.	Reduce likelihood of harm due to malice, error, or failure; reduce extent of harm.
Plan and manage diversity.	Reduce likelihood of harm due to malice, error, or failure; reduce extent of disruption.
Maintain redundancy.	Reduce likelihood of harm due to malice, error, or failure; reduce extent of disruption or degradation.
Make resources location-versatile.	Reduce likelihood of occurrence of adversarial events; reduce extent of disruption or degradation.
Leverage health and status data.	Reduce likelihood of harm due to malice, error, or failure by enabling response to changes in system state; reduce extent of harm by enabling detection of and response to indicators of damage.
Maintain situational awareness.	Reduce likelihood of harm due to malice, error, or failure by enabling response to indicators; reduce extent of harm by enabling detection of and response to indicators of damage.
Manage resources (risk-) adaptively.	Reduce likelihood of harm due to malice, error or failure by enabling response to changes in the operational environment; reduce extent of harm.
Maximize transience.	Reduce likelihood of occurrence by reducing the time during which an adverse event could occur; reduce likelihood of harm due to malice, error, or failure by reducing the time during which an event could result in harm.
Determine ongoing trustworthiness.	Reduce likelihood of harm due to corrupted, modified, or fabricated information by enabling untrustworthy information to be identified; reduce extent of harm by reducing the propagation of untrustworthy information.
Change or disrupt the attack surface.	Reduce likelihood of occurrence by removing the circumstances in which an adversarial event is feasible; reduce likelihood of harm due to adversarial events by making such events ineffective.
Make the effects of deception and unpredictability user-transparent.	Reduce the likelihood of occurrence of error; when Deception techniques are applied, reduce the likelihood of occurrence of adversarial events.

[44] 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.

Sections F.2.1 through F.2.14 provide more detailed descriptions of the fourteen structural cyber resiliency principles.

F.2.1 LIMIT THE NEED FOR TRUST

Trustworthiness can be defined as an entity 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 can be 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.

Application of this design principle is most effective early in the system life cycle, where 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 to the system's 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 component are not automatically propagated to classes or instances created from the original one. While limitations on inheritance can increase the burden on developers or administrators initially, 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.

F.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. Visibility of data can be controlled by such mechanisms as encryption, data hiding, or data obfuscation. Visibility of how some resources are used can also be controlled directly, for example, 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, including for example, 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 [MITRE16]. To limit visibility or to 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 which 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. Assignment of privileges ideally should reflect judgments of operational need (e.g., need-to-know, need-to-use) as well as trustworthiness. 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, communications channels, processes, 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.

F.2.3 CONTAIN AND EXCLUDE BEHAVIORS

The behavior of a system element, including what resources it uses, which system elements it interacts with, or when it takes a given action, can vary based on many legitimate circumstances. However, analysis of the mission or business functions (and the mission/business processes that carry out those missions and functions [NIST 800-39]), can identify some behaviors which are always unacceptable, and others which are acceptable only under specific circumstances. Thus, excluding behaviors prevents such behaviors 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 which can be affected by the behavior of a given system element. Such restriction can, but does not have to, 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.

F.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 [NIST 800-160, Vol. 1]. Multiple mechanisms to achieve the same objective or to 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 which could result in errors or vulnerabilities, such (multiple) mechanisms should be managed consistently.

Layering of defenses restricts the adversary's movement vertically in a layered 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). It can also serve to Contain and exclude behaviors. Partitioning can be based on administration and policy, as in security domains [NIST 800-160, Vol. 1], or can be guided and informed by the missions or business functions the system elements in the partition support. Partitions can be implemented physically or logically, at the network layer and 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.

F.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 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 which provide the same functionality can be used.

Multiple approaches to diversity can be identified. These include architectural diversity; design diversity; synthetic (or automated) diversity;[45] information diversity; diversity of command, control, and communications (C3) paths (including out-of-band communications); supply chain diversity [NIST 800-160, Vol. 1, Bodeau15]; geographic diversity;[46] 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. 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 translates into increased system life cycle costs.[47] This can also increase the risks 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 which reuse 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. And finally, the effectiveness of

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

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

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

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

Therefore, this design principle calls for the use of Diversity in system architecture and design to take manageability into consideration. It also calls for consideration of diversity in operational processes and practices, including non-cyber alternatives such as out-of-band measures [NIST 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, manageability, or both.

F.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 should be considered at multiple levels or layers in a layered architecture [Sterbenz14]. However, Redundancy when used in conjunction with Diversity, can increase complexity and present scalability challenges.

The extent of Redundancy should be established and maintained through analysis, looking 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—and it is also most effective in conjunction with the Plan and manage diversity and Layer and partition defenses structural principles.

F.2.7 MAKE RESOURCES LOCATION-VERSATILE

Location-versatile resources are those resources which do not require a fixed location, and which 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) using database sharding[48] (although this can present security challenges).

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

[48] 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.

virtualization (i.e., data management which 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 alternative reconstitution of mission capabilities, and diverse information sources can be used for 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 used 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.

F.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 hence of monitoring policy compliance (e.g., auditing or alerting on unauthorized access attempts). However, most system components provide health and status data to indicate component availability or unavailability for use. These include, for example, 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 those components can allocate and scale resources more effectively. Correlation of 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 [NIST 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.

F.2.9 MAINTAIN SITUATIONAL AWARENESS

For cybersecurity and cyber resiliency, situational awareness encompasses awareness of *system elements*, *threats*, and *mission dependencies* on system elements.[49] Awareness of system elements can rely on security status assessment, security monitoring, and performance monitoring, and can be achieved in conjunction with the Leverage health and status data design principle. Awareness of threats involves ingesting and using threat intelligence, recognizing that adversaries evolve. Awareness of system elements and of threats (via gathered data, correlated data, and processing capabilities) can be centralized or distributed, and can be enterprise-internal or cross-enterprise (e.g., via a managed security service provider).

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

[49] 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]."

during mission operations by tracking and analyzing resource use. This more dynamic approach supports agility and adaptability, and supports 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.

F.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) providing such functionality 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, repurposing resources); and discarding or isolating suspected system elements (e.g., terminating a service or locking out a user account, quarantining processing, diverting communications to a deception environment). 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), 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 which change the risk posture of the system, the mission, or business function it supports. Alternately, strategies can be applied unpredictably to address unknown risks.

F.2.11 MAXIMIZE TRANSIENCE

Non-persistence is a strategy to Reduce attack surfaces in the temporal dimension. Virtualization technologies, which simulate the hardware and/or software on which other software executes [NIST 800-125], 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 (processes, files, connections) need to be expunged (i.e., removed in such a way that no data remains on the shared resources).[50] If an executing process or service has been compromised by malicious software which changes its behavior or corrupts the data it offers to other system elements, expunging it, either by bringing it down or by moving it

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

and deleting the prior instance, also expunges the compromise. This can be done in response to suspicious behavior, or can be deliberately unpredictable.

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

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, for example, gold copies of software and configuration data; policy data for network function virtualization; and data quality validation as part of data virtualization.

F.2.12 DETERMINE ONGOING TRUSTWORTHINESS

In the *Control* phase of the cyber-attack life cycle [MITRE16], 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 *Execute* and *Maintain* phases of the cyber-attack life cycle. Periodic or ongoing validation can detect the effects of adversary activities before those effects become too significant or irremediable.

A variety of Substantiated Integrity mechanisms can be used to identify suspicious changes. Changes can be to properties or to behavior. Some behaviors, for example, 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, for example, processor, memory, disk use, or network use 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 processing, transmission, and storage overhead. Therefore, this structural principle is most effective in support of the Focus on common critical assets strategic principle.

Ideally, any system element which cannot be determined to be trustworthy 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.

F.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—for example, execution of a service can be moved from one platform or virtual machine to another. This approach, which leverages the Dynamic Positioning design principle, 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 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 which 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, it 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 unpredictability and deception user-transparent structural principle.

F.2.14 MAKE DECEPTION AND UNPREDICTABILITY EFFECTS USER-TRANSPARENT

Deception and unpredictability are intended to increase the adversaries' uncertainty about the system's structure and behavior; about what effects an adversary might be able to achieve; and about what actions cyber defenders might take in response to suspected malicious cyber 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 characteristics, structure, or behavior. 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 structure (e.g., dynamically changing partitions or isolating components) undermines the adversary's reconnaissance efforts. Unpredictable behavior (e.g., response latency) increases uncertainty about effects and about whether system behavior indicates defender awareness of malicious cyber activities. Unpredictability and deception can be applied separately, as well as synergistically. These two techniques can be highly effective against advanced adversaries. However, deception and unpredictability, if implemented poorly, 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 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.

APPENDIX G

CONTROLS SUPPORTING CYBER RESILIENCY

NIST SPECIAL PUBLICATION 800-53 SECURITY CONTROLS RELATED TO CYBER RESILIENCY

The methodology for determining whether a control[51] in [NIST 800-53][52] directly supports cyber resiliency is outlined below. It considers several factors. 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 be considered good cybersecurity practices in principle 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 [NIST 800-53], the following questions were used to identify controls supporting cyber resiliency.

- Is the control *primarily* focused on helping the system achieve a level of confidentiality, integrity, or availability[53] in situations where threats are considered *other than advanced persistent threats*? 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 per se.
- Is the control *primarily* focused on ensuring 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, the mapping to a technique is relatively straightforward. For example, some controls such as SC-26 (Honeypots) and SC-30 (Concealment and Misdirection) clearly map to the Deception technique. In other instances, the mapping is not as straightforward. Controls that do not map to a cyber resiliency technique[54] should generally not be considered controls supporting cyber resiliency.
- Does the control map to one of the cyber resiliency approaches[55] 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 detailed analysis of the controls and a control that maps to an approach is *likely* to be a resiliency control.

[51] For the remainder of this appendix, the term *control i*ncludes both controls and control enhancements.

[52] References to security controls in this appendix are taken from NIST Special Publication 800-53, Revision 4. The control references will be updated upon final publication of NIST Special Publication 800-53, Revision 5.

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

[54] The cyber resiliency techniques may change over time as both adversary and defender technology changes. A control may exist in [NIST 800-53] that supports cyber resiliency in a way not captured by the cyber resiliency techniques.

[55] Cyber resiliency *techniques* are general categories of related technologies, processes, and concepts. Within each technique, specific combinations of technologies, processes, and concepts (i.e., sub-categories) can be identified and referred to as cyber resiliency *approaches*.

Many of the controls in [NIST 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 supporting 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 advanced persistent threat should be identified as a cyber resiliency control.

- **Training controls (largely confined to AT family)**

  In general, training-related controls do not satisfy the conditions listed above.

- **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 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 generally are 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), and System and Communications Protection (SC) families have a high percentage of controls that are cyber resiliency-oriented. However, controls supporting 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 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-3) are considered basic information security measures, not cyber resiliency measures.

- One area where there is likely to be some confusion is between Auditing (Security Hygiene) and Analytic Monitoring (Resiliency). Controls that are focused on correlation of collected information are more likely to be Analytic Monitoring-focused. Controls 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 some instances, the distinguishing feature is not the control's mitigation mechanism or process, but rather where it is located or focused. For example, Boundary Protection (SC-7) is generally considered a preventative control focused on keeping adversaries out of the system or organization, and thus it is not considered a cyber resiliency control. But the same control implemented internal to the system in support of Segmentation is considered a resiliency control. Fortunately, SC-7 has three control enhancements (CEs) 20, 21, and 22—that are clearly internally focused so those CEs could be selected for providing cyber resiliency but others would not.

Finally, in many instances, cyber resiliency capabilities are reflected in control enhancements instead of base controls. In those situations, [NIST 800-53] requires that a parent control be selected if one or more of its controls enhancement 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 G-1 identifies the set of security controls and control enhancements in [NIST 800-53] that support cyber resiliency using the criteria outlined above. The table will be updated as new versions of the NIST control catalog are published.

TABLE G-1: NIST 800-53 CONTROLS SUPPORTING CYBER RESILIENCY AND RELEVANT TECHNIQUES

CONTROL NO.	CONTROL OR CONTROL ENHANCEMENT NAME	RESILIENCY TECHNIQUE
Access Control		
AC-2 (6)	ACCOUNT MANAGEMENT | *DYNAMIC PRIVILEGE MANAGEMENT*	Privilege Restriction Adaptive Response
AC-2 (12)	ACCOUNT MANAGEMENT | *ACCOUNT MONITORING / ATYPICAL USAGE*	Analytic Monitoring
AC-3 (2)	ACCESS ENFORCEMENT | *DUAL AUTHORIZATION*	Privilege Restriction
AC-3 (9)	ACCESS ENFORCEMENT | *CONTROLLED RELEASE*	Privilege Restriction
AC-4 (2)	INFORMATION FLOW ENFORCEMENT | *PROCESSING DOMAINS*	Segmentation
AC-4 (3)	INFORMATION FLOW ENFORCEMENT | *DYNAMIC INFORMATION FLOW CONTROL*	Adaptive Response
AC-4 (8)	INFORMATION FLOW ENFORCEMENT | *SECURITY POLICY FILTERS*	Substantiated Integrity
AC-4 (21)	INFORMATION FLOW ENFORCEMENT | *PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS*	Segmentation
AC-6	LEAST PRIVILEGE	Privilege Restriction
AC-6 (1)	LEAST PRIVILEGE | *AUTHORIZE ACCESS TO SECURITY FUNCTIONS*	Privilege Restriction
AC-6 (2)	LEAST PRIVILEGE | *NON-PRIVILEGED ACCESS FOR NON-SECURITY FUNCTIONS*	Privilege Restriction
AC-6 (3)	LEAST PRIVILEGE | *NETWORK ACCESS TO PRIVILEGED COMMANDS*	Privilege Restriction
AC-6 (4)	LEAST PRIVILEGE | *SEPARATE PROCESSING DOMAINS*	Privilege Restriction

CONTROL NO.	CONTROL OR CONTROL ENHANCEMENT NAME	RESILIENCY TECHNIQUE
AC-6 (5)	LEAST PRIVILEGE | *PRIVILEGED ACCOUNTS*	Privilege Restriction
AC-6 (6)	LEAST PRIVILEGE | *PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS*	Privilege Restriction
AC-6 (7)	LEAST PRIVILEGE | *REVIEW OF USER PRIVILEGES*	Privilege Restriction
AC-6 (8)	LEAST PRIVILEGE | *PRIVILEGE LEVELS FOR CODE EXECUTION*	Privilege Restriction
AC-6 (10)	LEAST PRIVILEGE | *PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*	Privilege Restriction
AC-12	SESSION TERMINATION	Non-Persistence
AC-23	DATA MINING PROTECTION	Analytic Monitoring
Audit		
AU-5 (3)	RESPONSE TO AUDIT PROCESSING FAILURES| *CONFIGURABLE TRAFFIC VOLUME THRESHOLDS*	Adaptive Response
AU-6 (3)	AUDIT REVIEW, ANALYSIS, AND REPORTING | *CORRELATE AUDIT REPOSITORIES*	Analytic Monitoring
AU-6 (5)	AUDIT REVIEW, ANALYSIS, AND REPORTING | *INTEGRATION / SCANNING AND MONITORING CAPABILITIES*	Analytic Monitoring
AU-6 (6)	AUDIT REVIEW, ANALYSIS, AND REPORTING | *CORRELATION WITH PHYSICAL MONITORING*	Analytic Monitoring
AU-6 (8)	AUDIT REVIEW, ANALYSIS, AND REPORTING | *FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS*	Privilege Restriction Analytic Monitoring Segmentation
AU-6 (9)	AUDIT REVIEW, ANALYSIS, AND REPORTING | *CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES*	Analytic Monitoring
AU-6 (10)	AUDIT REVIEW, ANALYSIS, AND REPORTING | *AUDIT LEVEL ADJUSTMENT*	Adaptive Response Analytic Monitoring
AU-7	AUDIT REDUCTION AND REPORT GENERATION	Analytic Monitoring
AU-9 (1)	PROTECTION OF AUDIT INFORMATION | *HARDWARE WRITE-ONCE MEDIA*	Substantiated Integrity
AU-9 (2)	PROTECTION OF AUDIT INFORMATION | *AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS*	Segmentation
AU-9 (3)	PROTECTION OF AUDIT INFORMATION | *CRYPTOGRAPHIC PROTECTION*	Substantiated Integrity
AU-9 (5)	PROTECTION OF AUDIT INFORMATION | *DUAL AUTHORIZATION*	Privilege Restriction
AU-15	ALTERNATE AUDIT CAPABILITY	Redundancy
Security Assessment and Authorization		
CA-8	PENETRATION TESTING	Analytic Monitoring
Configuration Management		
CM-2 (7)	BASELINE CONFIGURATION | *CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS*	Analytic Monitoring
CM-5 (3)	ACCESS RESTRICTIONS FOR CHANGE | *SIGNED COMPONENTS*	Substantiated Integrity
CM-5 (4)	ACCESS RESTRICTIONS FOR CHANGE | *DUAL-AUTHORIZATION*	Privilege Restriction
CM-5 (5)	ACCESS RESTRICTIONS FOR CHANGE | *LIMIT PRODUCTION / OPERATIONAL PRIVILEGES*	Privilege Restriction

CONTROL NO.	CONTROL OR CONTROL ENHANCEMENT NAME	RESILIENCY TECHNIQUE
CM-5 (6)	ACCESS RESTRICTIONS FOR CHANGE | *LIMIT LIBRARY PRIVILEGES*	Privilege Restriction
Contingency Planning		
CP-2 (5)	CONTINGENCY PLAN | *CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*	Coordinated Protection Dynamic Representation
CP-2 (8)	CONTINGENCY PLAN | *IDENTIFY CRITICAL ASSETS*	Dynamic Representation
CP-8 (3)	TELECOMMUNICATIONS SERVICES | *SEPARATION OF PRIMARY / ALTERNATE PROVIDERS*	Diversity
CP-9	INFORMATION SYSTEM BACKUP	Redundancy
CP-9 (6)	INFORMATION SYSTEM BACKUP | *REDUNDANT SECONDARY SYSTEM*	Redundancy
CP-9 (7)	INFORMATION SYSTEM BACKUP | *DUAL AUTHORIZATION*	Privilege Restriction
CP-11	ALTERNATE COMMUNICATIONS PROTOCOLS	Diversity
CP-12	SAFE MODE	Privilege Restriction Substantiated Integrity
CP-13	ALTERNATIVE SECURITY MECHANISMS	Redundancy Diversity Adaptive Response
Identification and Authentication		
IA-2 (6)	IDENTIFICATION AND AUTHENTICATION | *NETWORK ACCESS TO PRIVILEGED ACCOUNTS - SEPARATE DEVICE*	Coordinated Protection
IA-2 (7)	IDENTIFICATION AND AUTHENTICATION | *NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS – SEPARATE DEVICE*	Coordinated Protection
IA-2 (11)	IDENTIFICATION AND AUTHENTICATION | *REMOTE ACCESS - SEPARATE DEVICE*	Coordinated Protection
IA-2 (13)	IDENTIFICATION AND AUTHENTICATION | *OUT-OF-BAND AUTHENTICATION*	Coordinated Protection Segmentation Diversity
IA-10	ADAPTIVE IDENTIFICATION AND AUTHENTICATION	Adaptive Response Privilege Restriction
Incident Response		
IR-4 (2)	INCIDENT HANDLING | *DYNAMIC RECONFIGURATION*	Adaptive Response Dynamic Positioning
IR-4 (3)	INCIDENT HANDLING | *CONTINUITY OF OPERATIONS*	Adaptive Response Coordinated Protection
IR-4 (4)	INCIDENT HANDLING | *INFORMATION CORRELATION*	Coordinated Protection Analytic Monitoring
IR-4 (9)	INCIDENT HANDLING | *DYNAMIC RESPONSE CAPABILITY*	Adaptive Response
IR-4 (10)	INCIDENT HANDLING | *SUPPLY CHAIN COORDINATION*	Coordinated Protection
IR-10	INTEGRATED INFORMATION SECURITY ANALYSIS TEAM	Adaptive Response Analytic Monitoring Coordinated Protection
Maintenance		
MA-4 (4)	NONLOCAL MAINTENANCE | *AUTHENTICATION / SEPARATION OF MAINTENANCE SESSIONS*	Segmentation

CONTROL NO.	CONTROL OR CONTROL ENHANCEMENT NAME	RESILIENCY TECHNIQUE
Physical and Environmental Protection		
PE-3 (5)	PHYSICAL ACCESS CONTROL | *TAMPER PROTECTION*	Substantiated Integrity
PE-3 (6)	PHYSICAL ACCESS CONTROL | *FACILITY PENETRATION TESTING*	Analytic Monitoring
PE-6	MONITORING PHYSICAL ACCESS	Analytic Monitoring
PE-6 (2)	MONITORING PHYSICAL ACCESS | *AUTOMATED INTRUSION RECOGNITION / RESPONSES*	Analytic Monitoring Coordinated Protection
PE-6 (4)	MONITORING PHYSICAL ACCESS | *MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS*	Analytic Monitoring Coordinated Protection
PE-9 (1)	POWER EQUIPMENT AND CABLING | *REDUNDANT CABLING*	Redundancy
PE-11 (1)	EMERGENCY POWER | *LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY*	Redundancy
PE-11 (2)	EMERGENCY POWER | *LONG-TERM ALTERNATE POWER SUPPLY - SELF-CONTAINED*	Redundancy
PE-17	ALTERNATE WORK SITE	Redundancy
Planning		
PL-2 (3)	SYSTEM SECURITY PLAN | *PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES*	Coordinated Protection
PL-8 (1)	INFORMATION SECURITY ARCHITECTURE | *DEFENSE-IN-DEPTH*	Coordinated Protection
PL-8 (2)	INFORMATION SECURITY ARCHITECTURE | *SUPPLIER DIVERSITY*	Diversity
Risk Assessment		
RA-5 (5)	VULNERABILITY SCANNING | *PRIVILEGED ACCESS*	Analytic Monitoring Privilege Restriction
RA-5 (6)	VULNERABILITY SCANNING | *AUTOMATED TREND ANALYSES*	Analytic Monitoring
RA-5 (8)	VULNERABILITY SCANNING | *REVIEW HISTORIC AUDIT LOGS*	Analytic Monitoring
RA-5 (10)	VULNERABILITY SCANNING | *CORRELATE SCANNING INFORMATION*	Analytic Monitoring
System and Services Acquisition		
SA-11 (6)	DEVELOPER SECURITY TESTING AND EVALUATION | *ATTACK SURFACE REVIEWS*	Realignment
SA-12	SUPPLY CHAIN PROTECTION	Substantiated Integrity
SA-12 (1)	SUPPLY CHAIN PROTECTION | *ACQUISITION STRATEGIES / TOOLS / METHODS*	Substantiated Integrity Redundancy
SA-12 (5)	SUPPLY CHAIN PROTECTION | *LIMITATION OF HARM*	Diversity
SA-12 (10)	SUPPLY CHAIN PROTECTION | *VALIDATE AS GENUINE AND NOT ALTERED*	Substantiated Integrity
SA-12 (11)	SUPPLY CHAIN PROTECTION | *PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS*	Analytic Monitoring Substantiated Integrity
SA-12 (13)	SUPPLY CHAIN PROTECTION | *CRITICAL INFORMATION SYSTEM COMPONENTS*	Redundancy Diversity
SA-12 (14)	SUPPLY CHAIN PROTECTION | *IDENTITY AND TRACEABILITY*	Substantiated Integrity
SA-14	CRITICALITY ANALYSIS	Dynamic Representation Realignment

CONTROL NO.	CONTROL OR CONTROL ENHANCEMENT NAME	RESILIENCY TECHNIQUE
SA-15 (5)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | *ATTACK SURFACE REDUCTION*	Realignment
SA-17 (7)	DEVELOPER SECURITY ARCHITECTURE AND DESIGN | *STRUCTURE FOR LEAST PRIVILEGE*	Privilege Restriction
SA-18	TAMPER RESISTANCE AND DETECTION	Substantiated Integrity
SA-18 (1)	TAMPER RESISTANCE AND DETECTION | *MULTIPLE PHASES OF SDLC*	Substantiated Integrity
SA-18 (2)	TAMPER RESISTANCE AND DETECTION | *INSPECTION OF INFORMATION SYSTEMS, COMPONENTS, OR DEVICES*	Substantiated Integrity
SA-19	COMPONENT AUTHENTICITY	Substantiated Integrity
SA-20	CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS	Diversity
System and Communications Protection		
SC-3	SECURITY FUNCTION ISOLATION	Segmentation
SC-3 (1)	SECURITY FUNCTION ISOLATION | *HARDWARE SEPARATION*	Segmentation
SC-3 (2)	SECURITY FUNCTION ISOLATION | *ACCESS / FLOW CONTROL FUNCTIONS*	Segmentation
SC-3 (3)	SECURITY FUNCTION ISOLATION | *MINIMIZE NON-SECURITY FUNCTIONALITY*	Realignment
SC-3 (5)	SECURITY FUNCTION ISOLATION | *LAYERED STRUCTURES*	Realignment
SC-7 (10)	BOUNDARY PROTECTION | *UNAUTHORIZED EXFILTRATION*	Analytic Monitoring Non-persistence
SC-7 (11)	BOUNDARY PROTECTION | *RESTRICT INCOMING COMMUNICATIONS TRAFFIC*	Substantiated Integrity Privilege Restriction
SC-7 (13)	BOUNDARY PROTECTION | *ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS*	Segmentation
SC-7 (15)	BOUNDARY PROTECTION | *ROUTE PRIVILEGED NETWORK ACCESSES*	Realignment Segmentation Privilege Restriction
SC-7 (20)	BOUNDARY PROTECTION | *DYNAMIC ISOLATION / SEGREGATION*	Segmentation Adaptive Response
SC-7 (21)	BOUNDARY PROTECTION | *ISOLATION OF INFORMATION SYSTEM COMPONENTS*	Segmentation
SC-7 (22)	BOUNDARY PROTECTION | *SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS*	Segmentation
SC-8 (1)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY | *CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION*	Substantiated Integrity
SC-8 (4)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY | *CONCEAL / RANDOMIZE COMMUNICATIONS*	Deception Unpredictability
SC-10	NETWORK DISCONNECT	Non-Persistence
SC-23 (3)	SESSION AUTHENTICITY | *UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION*	Unpredictability
SC-25	THIN NODES	Privilege Restriction Non-persistence
SC-26	HONEYPOTS	Deception Analytic Monitoring

CONTROL NO.	CONTROL OR CONTROL ENHANCEMENT NAME	RESILIENCY TECHNIQUE
SC-28 (1)	PROTECTION OF INFORMATION AT REST | *CRYPTOGRAPHIC PROTECTION*	Substantiated Integrity
SC-29	HETEROGENEITY	Diversity
SC-29 (1)	HETEROGENEITY | *VIRTUALIZATION TECHNIQUES*	Diversity
SC-30	CONCEALMENT AND MISDIRECTION	Deception
SC-30 (2)	CONCEALMENT AND MISDIRECTION | *RANDOMNESS*	Unpredictability
SC-30 (3)	CONCEALMENT AND MISDIRECTION | *CHANGE PROCESSING / STORAGE LOCATIONS*	Dynamic Positioning Unpredictability
SC-30 (4)	CONCEALMENT AND MISDIRECTION | *MISLEADING INFORMATION*	Deception
SC-30 (5)	CONCEALMENT AND MISDIRECTION | *CONCEALMENT OF SYSTEM COMPONENTS*	Deception
SC-32	INFORMATION SYSTEM PARTITIONING	Segmentation
SC-34	NON-MODIFIABLE EXECUTABLE PROGRAMS	Substantiated Integrity
SC-34 (1)	NON-MODIFIABLE EXECUTABLE PROGRAMS | *NO WRITABLE STORAGE*	Non-Persistence
SC-34 (2)	NON-MODIFIABLE EXECUTABLE PROGRAMS | *INTEGRITY PROTECTION / READ-ONLY MEDIA*	Substantiated Integrity
SC-34 (3)	NON-MODIFIABLE EXECUTABLE PROGRAMS | *HARDWARE-BASED PROTECTION*	Substantiated Integrity
SC-35	HONEYCLIENTS	Analytic Monitoring Deception
SC-36	DISTRIBUTED PROCESSING AND STORAGE	Dynamic Positioning Redundancy
SC-36 (1)	DISTRIBUTED PROCESSING AND STORAGE | *POLLING TECHNIQUES*	Substantiated Integrity
SC-37	OUT-OF-BAND CHANNELS	Diversity
SC-39	PROCESS ISOLATION	Segmentation
SC-44	DETONATION CHAMBERS	Analytic Monitoring Deception
System and Information Integrity		
SI-3 (10)	MALICIOUS CODE PROTECTION | *MALICIOUS CODE ANALYSIS*	Analytic Monitoring
SI-4 (1)	INFORMATION SYSTEM MONITORING | *SYSTEM-WIDE INTRUSION DETECTION SYSTEM*	Analytic Monitoring
SI-4 (2)	INFORMATION SYSTEM MONITORING | *AUTOMATED TOOLS FOR REAL-TIME ANALYSIS*	Analytic Monitoring
SI-4 (3)	INFORMATION SYSTEM MONITORING | *AUTOMATED TOOL INTEGRATION*	Analytic Monitoring Adaptive Response
SI-4 (7)	INFORMATION SYSTEM MONITORING | *AUTOMATED RESPONSE TO SUSPICIOUS EVENTS*	Analytic Monitoring
SI-4 (10)	INFORMATION SYSTEM MONITORING | *VISIBILITY OF ENCRYPTED COMMUNICATIONS*	Analytic Monitoring
SI-4 (11)	INFORMATION SYSTEM MONITORING | *ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES*	Analytic Monitoring
SI-4 (16)	INFORMATION SYSTEM MONITORING | *CORRELATE MONITORING INFORMATION*	Analytic Monitoring Dynamic Representation

CONTROL NO.	CONTROL OR CONTROL ENHANCEMENT NAME	RESILIENCY TECHNIQUE
SI-4 (17)	INFORMATION SYSTEM MONITORING | *INTEGRATED SITUATIONAL AWARENESS*	Dynamic Representation
SI-4 (18)	INFORMATION SYSTEM MONITORING | *ANALYZE TRAFFIC / COVERT EXFILTRATION*	Analytic Monitoring
SI-4 (24)	INFORMATION SYSTEM MONITORING | *INDICATORS OF COMPROMISE*	Analytic Monitoring
SI-6	SECURITY FUNCTION VERIFICATION	Substantiated Integrity
SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	Substantiated Integrity
SI-7 (1)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | *INTEGRITY CHECKS*	Substantiated Integrity
SI-7 (5)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | *AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS*	Substantiated Integrity
SI-7 (6)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | *CRYPTOGRAPHIC PROTECTION*	Substantiated Integrity
SI-7 (7)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | *INTEGRATION OF DETECTION AND RESPONSE*	Substantiated Integrity Analytic Monitoring
SI-7 (9)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | *VERIFY BOOT PROCESS*	Substantiated Integrity
SI-7 (10)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | *PROTECTION OF BOOT FIRMWARE*	Substantiated Integrity Coordinated Protection
SI-7 (11)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | *CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES*	Privilege Restriction Segmentation
SI-7 (12)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | *INTEGRITY VERIFICATION*	Substantiated Integrity
SI-10 (5)	INFORMATION INPUT VALIDATION | *RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS*	Substantiated Integrity
SI-14	NON-PERSISTENCE	Non-Persistence
SI-14 (1)	NON-PERSISTENCE | *REFRESH FROM TRUSTED SOURCES*	Non-Persistence Substantiated Integrity
SI-15	INFORMATION OUTPUT FILTERING	Substantiated Integrity

APPENDIX H

RELATIONSHIPS AMONG CYBER RESILIENCY CONSTRUCTS

GOALS, OBJECTIVES, TECHNIQUES, APPROACHES, AND DESIGN PRINCIPLES

Section 3.1 presented the cyber resiliency constructs of goals, objectives, techniques, approaches, and design principles. Tables H-1 and H-2 illustrate that the mapping between goals and objectives is many to many, as are the mappings between techniques (including the approaches to implementing or applying techniques) and objectives.

TABLE H-1: CYBER RESILIENCY OBJECTIVES SUPPORT CYBER RESILIENCY GOALS

Goals / Objectives	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 H-2: TECHNIQUES AND IMPLEMENTATION APPROACHES TO ACHIEVE OBJECTIVES

Objectives / Techniques/Approaches	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	X		
Monitoring and Damage Assessment			X	X	X	X		
Sensor Fusion and Analysis						X		
Malware and Forensic Analysis						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

Objectives / Techniques/Approaches	Prevent Avoid	Prepare	Continue	Constrain	Reconstitute	Understand	Transform	Re-Architect
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			
Dynamic Representation		X	X		X	X		
Dynamic Mapping and Profiling		X				X		
Dynamic Threat Modeling						X		
Mission Dependency and Status Visualization		X	X		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				
Attribute-Based Usage Restriction	X				X			
Dynamic Privileges	X			X	X			
Realignment	X						X	X
Purposing	X							X
Offloading							X	X
Restriction							X	X

Objectives / Techniques/Approaches	Prevent Avoid	Prepare	Continue	Constrain	Reconstitute	Understand	Transform	Re-Architect
Replacement							X	X
Specialization							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 3.3 identifies cyber resiliency design principles. Strategic design principles support achieving cyber resiliency objectives as shown in Table H-3, while structural design principles provide guidance on how to apply cyber resiliency techniques as shown in Table H-4. Some techniques are required by a design principle; these are **bolded**. Others (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.

TABLE H-3: 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

TABLE H-4: 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**, **Dynamic Representation**, Substantiated Integrity
Maintain situational awareness.	Analytic Monitoring, **Dynamic Representation**
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
Make the effects of deception and unpredictability user-transparent.	Adaptive Response, **Coordinated Protection**, Deception, Unpredictability

APPENDIX I

CYBER RESILIENCY EFFECTS ON ADVERSARY ACTIVITIES

MANAGING RISK THROUGH THE APPLICATION OF CYBER RESILIENCY SOLUTIONS

Cyber resiliency solutions are relevant only if they have some effect on risk, specifically by reducing the likelihood of occurrence of threat events,[56] the ability of threat events to cause harm, and the extent of that harm.[57] The types of analysis of system architectures, designs, implementations, and operations indicated for cyber resiliency can include consideration of what effects alternatives could have on the threat events which 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 measures of effectiveness. Therefore, more specific classes of effects are defined:

- Deter, divert, and deceive in support of redirect;
- Prevent, preempt, and expunge in support of preclude;
- Contain, degrade and delay in support of impede;
- Shorten and recover in support of limit; and
- Detect, reveal, and scrutinize in support of expose.

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 redirect (including deter, divert, and deceive) apply to non-adversarial and adversarial threat events; redirect (including deter, divert and deceive) is applicable only to adversarial threat events.

Table I-1 illustrates how the use of certain approaches to implementing selected cyber resiliency techniques for protection against attack could have the identified effect. The term *defender* refers to the organization or to organizational staff 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 prevent, detect, or expunge. Table I-2 shows the potential effects of cyber resiliency techniques and approaches on adversarial threats. Table I-3 shows the potential effects of cyber resiliency techniques on risk with regard to impact, likelihood of impact, and likelihood of occurrence.

[56] The term *threat event* refers to an event or situation that has the potential for causing undesirable consequences or impact. 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.

[57] While many different risk models are potentially valid and useful, three elements are common across most models. These are: 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); 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 the *level of the impact* [NIST 800-30].

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

INTENDED EFFECT	EFFECT ON RISK	EXPECTED RESULT
Redirect (includes deter, divert, and deceive): Direct adversary activities away from defender-chosen targets.	Reduce likelihood of occurrence and, (to a lesser extent) reduce likelihood of impact.	• The adversary's efforts cease, or become misinformed. • The adversary targets incorrectly.
Deter: Discourage the adversary from undertaking further activities, by instilling fear (e.g., of attribution or retribution) or doubt that those activities would achieve intended effects (e.g., that targets exist).	Reduce 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. The result is that the adversary chooses to not launch attack due to fear of detection and reprisal.
Divert: Lead the adversary to direct activities away from defender-chosen targets.	Reduce likelihood of occurrence.	• The adversary refocuses activities on different targets (e.g., other organizations, defender-chosen alternate targets). • The adversary's efforts are wasted. **Example**: The defender uses selectively planted false information (disinformation) and honeynets (misdirection) to cause an adversary to focus its malware at virtual sandboxes, while at the same time employing obfuscation to hide the actual resources. The result is that the adversary's attacks are directed away from critical resources.
Deceive: Lead the adversary to believe false information about defended systems, missions, or organizations, or about defender capabilities or TTPs.	Reduce likelihood of occurrence and/or reduce likelihood of impact.	• The adversary's efforts are wasted, as the assumptions on which the adversary bases attacks are false. **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 nonexistent cybersecurity protections.
Preclude (includes expunge, preempt, and prevent): Ensure that specific threat events do not have an effect.	Reduce likelihood of occurrence and/or reduce likelihood of impact.	• The adversary's efforts or resources cannot be applied or are wasted.
Expunge: Remove unsafe, incorrect, or corrupted resources that could cause damage.	Reduce likelihood of impact of subsequent events in the same threat scenario.	• The adversary loses a capability for some period, as adversary-

INTENDED EFFECT	EFFECT ON RISK	EXPECTED RESULT
		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-per*sistent services) at random intervals (temporal unpredictability). As a result, the adversary's malware that is implanted in the software is expunged.
Preempt: Forestall or avoid conditions under which the threat event could occur or result in an effect.	Reduce likelihood of occurrence and/or reduce likelihood of impact.	• The adversary's resources cannot be applied and/or the adversary cannot perform activities (e.g., because resources are destroyed or made inaccessible). **Example:** Critical software is not assembled (adaptive management) or activated (non-persistent services) until it is needed. The adversary, therefore, cannot perform reconnaissance on, and tailor malware targeted to, the software.
Prevent: Create conditions under which the threat event cannot be expected to result in an effect.	Reduce likelihood of impact.	• 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. **Example:** Subtle variations in critical software are implemented (synthetic diversity), with the result that the adversary's malware is no longer able to compromise the targeted software.
Impede (includes contain, degrade and delay): Make it more difficult for threat events to cause adverse impacts or consequences.	Reduce likelihood of impact and reduce level of impact.	• To achieve the intended effects, the adversary should invest more resources or undertake additional activities.
Contain: Restrict the effects of the threat event to a limited set of resources.	Reduce level of impact.	• 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 detection of malware, with the result that the

INTENDED EFFECT	EFFECT ON RISK	EXPECTED RESULT
		effects of the malware is limited to just initially infected enclaves.
Degrade: Decrease the likelihood that a given threat event will have a given level of effectiveness or impact.	Reduce likelihood of impact and reduce level of impact.	• The adversary achieves some but not all intended effects. • The adversary achieves all intended effects but only after taking additional actions. **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 that is targeted at specific software can only compromise a subset of the targeted systems; a sufficient number continue to operate to keep mission going, although in degraded mode.
Delay: Increase the amount of time needed for a threat event to result in adverse impacts.	Reduce likelihood of impact and reduce level of impact.	• The adversary achieves the intended effects, but may not achieve them within the intended period. • The adversary's activities may, therefore, be exposed to greater risk of detection and analysis. **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 with increased frequency for more critical resources. The result is that it takes the attacker more time to successfully compromise the targeted resources.
Limit (includes shorten and recover): Restrict the consequences of threat events by limiting the damage or effects they cause in terms of time, system resources, and/or mission or business impacts.	Reduce level of impact and reduce likelihood of impact of subsequent events in the same threat scenario.	• The adversary's effectiveness is limited.
Shorten: Limit the duration of a threat event or the conditions caused by a threat event.	Reduce level of impact.	• The time period during which the adversary's activities have their intended effects 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

INTENDED EFFECT	EFFECT ON RISK	EXPECTED RESULT
		causes it to shut down, the defender can increase its use of the other suppliers, thus shortening the time when it is without the critical components.
Recover: Roll back the consequences of a threat event, particularly with respect to mission or business impairment.	Reduce level of impact.	• The adversary fails to retain mission or business impairment due to recovery of the capability to perform key missions or business operations. **Example**: Resources determined to be corrupted or suspect (integrity checks, behavior validation) are restored from a clean copy (protected backup and restore).
Expose (includes detect, scrutinize and reveal): Reduce risk due to ignorance of threat events and possible replicated or similar threat events in the same or similar environments.	Reduce likelihood of impact.	• The adversary loses the advantage of stealth, as defenders are better prepared by developing and sharing threat intelligence.
Detect: Identify threat events or their effects by discovering or discerning the fact that an event is occurring, has occurred, or (based on indicators, warnings, and precursor activities) is about to occur.	Reduce likelihood of impact and reduce 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, particularly with respect to patterns of exploiting vulnerabilities, predisposing conditions, and weaknesses, to inform more effective detection and risk response.	Reduce likelihood of impact.	• The adversary loses the advantages of uncertainty, confusion, and doubt. • The defender understands the adversary better, based on analysis of adversary activities, including the artifacts (e.g., malicious code) and effects associated with those activities and on 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 defender, allowing the defender to apply their TTPs in a safe environment. The defender then analyzes (malware and

INTENDED EFFECT	EFFECT ON RISK	EXPECTED RESULT
		forensic analysis) the malware captured in the honeynet to determine the nature of the attacker's TTPs, allowing it to develop appropriate defenses.
Reveal: Increase awareness of risk factors and relative effectiveness of remediation approaches across the stakeholder community, to support common, joint, or coordinated risk response.	Reduce likelihood of impact, particularly in the future.	• The adversary loses the advantage of surprise and possible 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, which 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).

TABLE I-2: EFFECTS OF CYBER RESILIENCY TECHNIQUES AND APPROACHES ON ADVERSARIAL THREATS

TECHNIQUES AND APPROACHES	EFFECTS ON ADVERSARIAL THREATS
Adaptive Response	Contain, Degrade, Delay, Prevent, Recover, Reveal, Shorten
Dynamic Reconfiguration	Degrade, Delay, Prevent, Reveal, Shorten, Recover
Dynamic Resource Allocation	Degrade, Delay, Prevent, Reveal, Shorten, Recover
Adaptive Management	Contain, Degrade, Delay, Prevent, Reveal, Shorten, Recover
Analytic Monitoring	Detect, Scrutinize
Monitoring and Damage Assessment	Detect, Scrutinize
Sensor Fusion and Analysis	Detect
Malware and Forensic Analysis	Scrutinize
Coordinated Protection	Degrade, Delay, Detect
Calibrated Defense-in-Depth	Degrade, Delay
Consistency Analysis	Detect
Orchestration	Detect
Self-Challenge	Detect, Scrutinize
Deception	Scrutinize, Deceive, Degrade, Delay, Detect, Deter, Divert
Obfuscation	Deceive, Degrade, Delay

TECHNIQUES AND APPROACHES	EFFECTS ON ADVERSARIAL THREATS
Disinformation	Deceive, Degrade, Delay, Deter, Divert
Misdirection	Scrutinize, Deceive, Degrade, Delay, Detect, Divert
Tainting	Deceive, Degrade, Detect, Divert
Diversity	Contain, Degrade, Delay, Prevent, Recover
Architectural Diversity	Contain, Degrade, Delay, Prevent, Recover
Design Diversity	Contain, Degrade, Delay, Prevent, Recover
Synthetic Diversity	Degrade, Delay, Prevent
Information Diversity	Degrade, Delay, Prevent, Recover
Path Diversity	Contain, Degrade, Delay, Prevent, Recover
Supply Chain Diversity	Contain, Degrade, Delay, Prevent, Recover
Dynamic Positioning	Degrade, Delay, Detect, Divert, Preempt, Recover, Shorten
Functional Relocation of Sensors	Detect
Functional Relocation of Cyber Resources	Degrade, Delay, Divert, Preempt
Asset Mobility	Degrade, Delay, Divert, Preempt
Fragmentation	Degrade, Delay, Preempt, Recover, Shorten
Distributed Functionality	Degrade, Delay, Preempt, Recover, Shorten
Dynamic Representation	Scrutinize, Detect, Recover, Reveal
Dynamic Mapping and Profiling	Scrutinize, Detect
Dynamic Threat Modeling	Detect, Reveal
Mission Dependency and Status Visualization	Recover, Scrutinize, Detect
Non-Persistence	Degrade, Delay, Expunge, Preempt, Prevent, Shorten
Non-Persistent Information	Degrade, Delay, Preempt, Prevent
Non-Persistent Services	Degrade, Delay, Expunge, Preempt, Prevent, Shorten
Non-Persistent Connectivity	Degrade, Delay, Preempt, Prevent
Privilege Restriction	Contain, Degrade, Delay, Prevent
Trust-Based Privilege Management	Contain, Degrade, Delay, Prevent
Attribute-Based Usage Restriction	Contain, Degrade, Delay, Prevent
Dynamic Privileges	Contain, Degrade, Delay, Prevent
Realignment	Contain, Degrade, Delay, Prevent
Purposing	Degrade, Delay, Prevent
Offloading	Contain, Degrade, Delay, Prevent
Restriction	Contain, Degrade, Delay, Prevent
Replacement	Degrade, Delay, Prevent
Specialization	Degrade, Delay, Prevent
Redundancy	Degrade, Recover, Shorten
Protected Backup and Restore	Recover, Shorten
Surplus Capacity	Degrade, Recover, Shorten
Replication	Degrade, Recover, Shorten
Segmentation	Contain, Degrade, Delay
Predefined Segmentation	Contain, Degrade, Delay

TECHNIQUES AND APPROACHES	EFFECTS ON ADVERSARIAL THREATS
Dynamic Segmentation and Isolation	Contain, Degrade, Delay
Substantiated Integrity	Detect, Prevent, Recover, Shorten
Integrity Checks	Detect, Prevent
Provenance Tracking	Detect, Prevent, Shorten
Behavior Validation	Detect, Prevent, Recover, Shorten
Unpredictability	Delay, Detect, Prevent, Shorten
Temporal Unpredictability	Delay, Detect, Prevent, Shorten
Contextual Unpredictability	Delay, Detect, Prevent, Shorten

TABLE I-3: 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	
Coordinated Protection	X	X	
Deception		X	X
Diversity	X	X	
Dynamic Positioning	X	X	X
Dynamic Representation	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	

APPENDIX J

MITIGATING ADVANCED PERSISTENT THREATS

APPLYING CYBER RESILIENCY CONCEPTS TO COUNTER ADVERSARY TACTICS AND TECHNIQUES

The primary focus of cyber resiliency is to counter attacks on systems from the APT. One way to better understand how that is done is to combine the cyber resiliency engineering framework with a taxonomy of threat events. This appendix illustrates how certain cyber resiliency techniques and approaches can affect threat events, using the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) framework for categorizing adversary activities in [MITRE16]. The threat framework facilitates modeling the post-compromise behavior of an adversary seeking to exfiltrate sensitive information at a granular level. In so doing, the framework "serves as both the adversary emulation playbook and as a method for discovering analytic coverage and defense gaps inside a target network [Strom17]."

For implementation-neutrality and brevity, this appendix focuses on ten categories or tactics of the APT: *Persistence*, *Privilege Escalation*, *Defense Evasion*, *Credential Access*, *Discovery*, *Lateral Movement*, *Execution*, *Collection*, *Exfiltration*, and *Command and Control*. For each of the categories, a representative analysis identifies the specific cyber resiliency techniques and implementation approaches which could mitigate (i.e., reduce the likelihood of success or the severity of consequences of) methods in that category. The analysis includes a short discussion of the potential effect or effects (as defined in Appendix I) which the technique and approach would have on the adversary tactic (i.e., on most or all of the individual methods in that category). The identification and discussion of the cyber resiliency techniques and implementation approaches presented in Tables J-1 through J-10 are intended to be representative, illustrating how the analysis is carried out. Additional cyber resiliency techniques or approaches can be identified to mitigate adversary tactics in a variety of systems and environments of operation.

TABLE J-1: CYBER RESILIENCY TECHNIQUES AND APPROACHES FOR PERSISTENCE

PERSISTENCE	
Persistence refers to any access, action, or configuration change to a system that gives an adversary a persistent presence on that system. Adversaries will often need to maintain access to systems through interruptions such as system restarts, loss of credentials, or other failures.	
TECHNIQUE: Adaptive Response	
APPROACH: Dynamic Reconfiguration	Making changes to certain resources that the adversary is known to employ (e.g., configuration files) renders the adversary's knowledge of resources and configuration outdated. As a result, the adversary's actions are impeded, making it more difficult for the adversary to maintain its persistent position in the organization's infrastructure. In addition, resource reallocation may result in the removal of resources from the adversary's control that it uses to remain hidden, thus increasing the likelihood that it will be detected. In addition, reconfiguration (e.g., changing internal communications or call paths) renders the adversary's stealthy means of communication ineffective, aiding in revealing the adversary.
TECHNIQUE: Diversity	
APPROACH: Architectural Diversity	The adversary's efforts at persisting are geared toward specific operating systems and architectures (e.g., Windows vs. Linux). The efforts will not work against variant implementations as such implementations are different from the implementations the adversary anticipated (e.g., tools the adversary needs to compromise Windows-based systems are different than those tools needed to compromise Linux-based systems, and therefore adversary will need different tools than originally in its toolset). This will prevent the adversary from establishing a stealthy, persistent presence. Moreover, the failure of the adversary's techniques to achieve a foothold (because it is designed for a specific architecture) will also increase the likelihood that the adversary's presence will be detected. Any effort by the adversary to develop tools capable of compromising all of the architectural designs will cost the adversary additional time and resources, thus delaying the adversary's ability to compromise the resources in a timely manner.
TECHNIQUE: Non-Persistence	
APPROACH: Non-Persistent Services	The adversary's attempt to exploit a vulnerability to achieve a persistent foothold is impeded if the attacked service is terminated because it is no longer needed by the defender. Moreover, if re-instantiated from a clean version, the new instance of the service will not be compromised and malware will no longer exist. Any persistent foothold established by the adversary is eliminated and the adversary is effectively flushed from its foothold. Even if a foothold is not eliminated, the restart of the service could create indicators of persistence, facilitating detection.

TABLE J-2: CYBER RESILIENCY TECHNIQUES AND APPROACHES FOR PRIVILEGE ESCALATION

PRIVILEGE ESCALATION
Privilege Escalation refers to the methods that allow an adversary to obtain a higher level of permissions on a system or network. Certain tools or actions require a higher level of privilege to work and are likely necessary at many points throughout a remote operation.
TECHNIQUE: Analytic Monitoring

PRIVILEGE ESCALATION	
APPROACH: Monitoring and Damage Assessment	A defender can increase probability of detection of an adversary through monitoring of privilege states, movement and integrity of access tokens, unusual privilege changes, or malfunction of privilege management actions, making the adversary's activities visible to defenders.
TECHNIQUE: Privilege Restriction	
APPROACH: Trust-Based Privilege Management	Strict management and diligence in monitoring of privileges is a fundamental method to delay, degrade, or curtail attacker-attempted privilege escalation (e.g., dividing privileges among more administrators, auditing any changes for consistency against entity roles).
APPROACH: Dynamic Privileges	This approach impedes, delays, or degrades adversary actions since the adversary must pass additional contextual tests, or take additional time to accomplish escalation given transient permissions, such as required to change configuration settings or installation of software.
TECHNIQUE: Substantiated Integrity	
APPROACH: Behavior Validation	Continuous validation of privilege change actions can lead to early detection of attacker compromises, such as noting unexpected software execution in a non-application context.

TABLE J-3: CYBER RESILIENCY TECHNIQUES AND APPROACHES FOR DEFENSE EVASION

DEFENSE EVASION	
Defense Evasion refers to the methods an adversary may use for the purpose of evading detection or avoiding other defenses.	
TECHNIQUE: Analytic Monitoring	
APPROACH: Sensor Fusion and Analysis	Sensors placed at various locations where the adversary is known to attempt to hide may detect anomalous behavior at these locations, although not necessarily detecting the adversary. But detection of anomalies at multiple locations could indicate adversary activity and is something that only the fusion of the sensor data would reveal.
APPROACH: Malware and Forensic Analysis	The adversary's efforts at evasion may, in some instances, result in leaving behind artifacts of past movement or location. Analysis of such artifacts may provide clues as to the adversary's current whereabouts, facilitating detection.
TECHNIQUE: Non-Persistence	
APPROACH: Non-Persistent Services	If compromised services that the adversary is employing in support of its evasion are terminated when no longer needed and if such services are re-instantiated from a clean version, then the new instances will not be compromised; malware will be expunged, and the adversary's activities will be impeded.
TECHNIQUE: Realignment	
APPROACH: Restriction	The removal or disabling of unneeded and risky functionality from services will delay and degrade the ability of the adversary to compromise such services and use the services to evade detection. Potentially, the removal of unneeded functionality (e.g., removing PSEXEC.EXE from Windows systems) may prevent the adversary from compromising the services and prevent it from successfully continuing evasion.

DEFENSE EVASION	
TECHNIQUE: Substantiated Integrity	
APPROACH: Integrity Checks	The organization can replace polynomial hashes on files with cryptographically signed hashes. Such actions may prevent typical binary padding attacks causing the adversary to work harder (find alternate places to hide) and detect efforts by adversary to circumvent non-crypto hashes.

TABLE J-4: CYBER RESILIENCY TECHNIQUES AND APPROACHES FOR CREDENTIAL ACCESS

CREDENTIAL ACCESS	
Credential Access refers to methods resulting in access to, or control over, a system, a domain, or service credentials that are used within an enterprise environment.	
TECHNIQUE: Coordinated Protection	
APPROACH: Calibrated Defense-in-Depth	By mandating the use of different sets of credentials to gain access to highly sensitive or critical resources, the defender imposes additional time and/or effort on the adversary, delaying and degrading its chances of achieving its aim.
TECHNIQUE: Deception	
APPROACH: Obfuscation	The use of obfuscation measures such as encryption impedes adversary activities to obtain credentials. For example, storing passwords in encrypted files requires greater work by the adversary to extract or guess those passwords.
TECHNIQUE: Diversity	
APPROACH: Path Diversity	Use of means such as out-of-band communication channels to transmit portions of a credential can potentially impede adversary activities to successfully compromise the entire credential.

TABLE J-5: CYBER RESILIENCY TECHNIQUES AND APPROACHES FOR DISCOVERY

DISCOVERY	
Discovery refers to methods that allow an adversary to gain knowledge about a system and its internal network.	
TECHNIQUE: Adaptive Response	
APPROACH: Dynamic Reconfiguration	This approach limits the useful life (age) on the gathered information. The adversary's exploit is based on outdated premises, curtailing impact of the adversary actions.
TECHNIQUE: Deception	
APPROACH: Obfuscation	Use of encryption or other means to hide targets of interest to the adversary can delay and degrade adversary actions needed to deduce the value or location of possible targets. As a result, the adversary must try to cover more target area than necessary to decide on specific targets and perform the data collection. In addition, use of encryption causes additional delay, both from decryption and from confusing adversaries on what information may be of interest.

DISCOVERY	
APPROACH: Disinformation	The deceived adversary wastes time and resources towards a fabricated, erroneous picture of the environment, of its mission, topology, and/or asset. Moreover, when applying this false information, the chances of the adversary being detected increases.
TECHNIQUE: Non-Persistence	
APPROACH: Non-Persistent Information	Retaining information for the minimum time necessary curtails adversary benefits from information discovery and increases work needed to obtain the information, impeding additional activities.

TABLE J-6: CYBER RESILIENCY TECHNIQUES AND APPROACHES FOR LATERAL MOVEMENT

LATERAL MOVEMENT	
Lateral Movement refers to methods that enable an adversary to access and control remote systems on a network. Often the next step for lateral movement is remote execution of tools introduced by an adversary.	
TECHNIQUE: Coordinated Protection	
APPROACH: Calibrated Defense-in-Depth	This approach contains, degrades, or delays the adversary's ability to move from one system resource to another by requiring the adversary to circumvent multiple defensive mechanisms.
TECHNIQUE: Diversity	
APPROACH: Architectural Diversity, Design Diversity, Synthetic Diversity	The diverse implementation of system components may require an adversary to invest time and resources in developing lateral movement methods tailored to the different architectures, thus delaying or degrading adversary activities.
TECHNIQUE: Dynamic Positioning	
APPROACH: Asset Mobility	This approach delays lateral movement by changing location of a targeted resource, causing the adversary to expend more time and effort.
TECHNIQUE: Non-Persistence	
APPROACH: Non-Persistent Connectivity	By limiting the duration of (and in some instances eliminating) network connections, lateral adversary movement is delayed, degraded, or possibly prevented or curtailed as the adversary must expend additional time and effort trying (and possibly failing) to find alternate network connections.
TECHNIQUE: Segmentation	
APPROACH: Predefined Segmentation	Having the adversary traverse multiple boundaries and enclaves will impede the adversary's movement, requiring the adversary to work harder or take longer to achieve its desired lateral movement.

TABLE J-7: CYBER RESILIENCY TECHNIQUES AND APPROACHES FOR EXECUTION

EXECUTION
Execution refers to methods that result in execution of adversary-controlled code on a local or remote system.
TECHNIQUE: Adaptive Response

EXECUTION	
APPROACH: Dynamic Reconfiguration	Configuration changes (e.g., dynamic script usage change during execution of key processes) delay, prevent, or limit execution or require additional adversary attempts.
TECHNIQUE: Analytic Monitoring	
APPROACH: Monitoring and Damage Assessment	Monitoring detects adversary attempts or successful execution, containing or curtailing serious effects of the actions, such as execution of a PowerShell command where only production application code is expected.
TECHNIQUE: Diversity	
APPROACH: Architectural Diversity, Design Diversity, Synthetic Diversity	Diversity can delay or degrade adversary attempts to execute code, since the adversary's exploits will work only against a subset of the variant implementations.
TECHNIQUE: Unpredictability	
APPROACH: Temporal Unpredictability, Contextual Unpredictability	Making random changes to the environment causes the adversary to execute malware at the wrong time or in the wrong state, thus limiting the harm of any immediate or coordinated attacks.

TABLE J-8: CYBER RESILIENCY TECHNIQUES AND APPROACHES FOR COLLECTION

COLLECTION	
Collection refers to methods used to identify and gather information, such as sensitive files, from a target network prior to exfiltration.	
TECHNIQUE: Deception	
APPROACH: Misdirection	Deceiving the adversary will delay and degrade adversary actions through misdirecting adversary to false targets via deception environments that mimic common collection targets (e.g., drive shares, artificial databases or information entries). In addition, diverting the adversary to a virtual sandbox reveals the adversary's TTPs to the defender.
TECHNIQUE: Dynamic Positioning	
APPROACH: Fragmentation	Fragmenting information and distributing it to various locations impedes the adversary efforts to locate all of the targeted information and will cause the adversary to work harder as it tries to extract information for collection. The adversary's efforts may also become easier to detect.
TECHNIQUE: Segmentation	
APPROACH: Predefined Segmentation, Dynamic Segmentation and Isolation	Isolating information of high sensitivity or criticality in separate enclaves, delays adversary collection activities as the adversary tries to penetrate the enclaves' isolation mechanisms.

TABLE J-9: CYBER RESILIENCY TECHNIQUES AND APPROACHES FOR EXFILITRATION

EXFILTRATION	
Exfiltration refers to methods that result or aid in an adversary removing files and information from a target system. This category also covers locations on a system or network where an adversary may look for information to exfiltrate.	
TECHNIQUE: Analytic Monitoring	
APPROACH: Sensor Fusion and Analysis	Placement of sensors at multiple, known exfiltration points and then fusing the multiple sensor findings, increases the chances of detecting patterns of anomalous traffic, making the adversary's exfiltration efforts more visible to defenders.
TECHNIQUE: Deception	
APPROACH: Obfuscation	By the defender encrypting or otherwise hiding valuable information, the adversary cannot reliably determine which targets are valuable or cannot make the correlations needed to deduce the value of possible targets. Hence, the adversary must either try to exfiltrate more files than necessary to achieve its objectives, or accept more uncertainty as to its effectiveness. This impedes the ability of the adversary to selectively, effectively, and continually exfiltrate sensitive information without such efforts being detected.
APPROACH: Disinformation	By the defender seeding the set of valuable information with misleading or incorrect information, the exfiltration at worst provides little or no value to the adversary; at best the exfiltrated misinformation deceives the adversary into making incorrect assumptions in its future mission planning. Either way, the adversary's resources that are directed at acquiring and exfiltrating valuable information is to some extent wasted.
APPROACH: Tainting	The adversary exfiltrates information that has been modified so that it can alert the organization of its exfiltration. That aids the organization in detecting the exfiltration and possibly identifying the location of the adversary.
TECHNIQUE: Dynamic Positioning	
APPROACH: Functional Relocation of Sensors	Relocation of sensors to likely points of exfiltration increases the likelihood of detection and in so doing, impedes adversary efforts to continue such efforts while retaining a stealthy presence.

TABLE J-10: CYBER RESILIENCY TECHNIQUES AND APPROACHES FOR COMMAND AND CONTROL

COMMAND AND CONTROL	
Command and Control refers to methods an adversary uses to communicate with systems under its control within a target system including for example, using legitimate protocols such as HTTP to carry command and control information.	
TECHNIQUE: Non-Persistence	
APPROACH: Non-Persistent Connectivity	By limiting or disabling communication channels until they are needed, the period during which an adversary can make use of these channels for command and control becomes limited. This may force the adversary to employ less secure (from the adversary's perspective) communication channels, increasing the risk of detection or of having its TTPs revealed. Such

COMMAND AND CONTROL	
	measures can also delay the needed command and control communications or cause the adversary to work harder to maintain such communications.
TECHNIQUE: Realignment	
APPROACH: Replacement	Replacement can impede or prevent adversary command and control activities. An adversary may be unable to compromise a customized proxy server, thus eliminating that server as a command and control channel. Even if the customized proxy server does not completely stop the adversary, it will take the adversary additional time and resources to develop exploits against it or to find an alternate server to use for communications.
TECHNIQUE: Unpredictability	
APPROACH: Temporal Unpredictability	The inability to accurately predict the timing of defender's actions (e.g., when the defender will patch or upgrade out of cycle) affects the adversary's ability to compromise proxy servers, protocols, and communication channels while trying to continue its command and control activities. The unpredictable timing of the monitoring also increases the likelihood of detection.