MITRE

Cyber Resiliency and NIST Special Publication 800-53 Rev.4 Controls

Sponsor: NIST
Dept. No.: G020

Project No.: 19128454-CA

MTR130531

Bedford, MA

Deb Bodeau
Richard Graubart

September 2013

Abstract

Attacks in cyberspace are no longer limited to simple discrete events such as the spread of a virus or a denial-of-service attack against an organization. Campaigns are waged by the advanced persistent threat (APT), which has the capabilities, resources and persistence to breach even well patched and monitored IT infrastructures. Therefore, today's systems must be resilient against the APT. MITRE has developed its cyber resilience engineering framework (CREF) to support the development of structured and consistent cyber resiliency guidance. The CREF consists of goals, objectives and techniques. In the context of the Risk Management Framework defined by NIST SP 800-37, cyber resiliency techniques can be applied to a system, set of shared services, or common infrastructure by selecting, tailoring, and implementing security controls. This document identifies those controls in NIST SP 800-53R4 that support cyber resiliency.

This page intentionally left blank.

Table of Contents

List of Figures

List of Tables

1 Introduction

Missions, business functions, organizations, and nations are increasingly dependent on cyberspace. Attacks in cyberspace are no longer limited to simple (albeit significantly harmful) discrete events such as the spread of a virus or worm, or a denial-of-service attack against an organization. Campaigns are waged by the advanced persistent threat (APT), following a cyber attack lifecycle[1] as illustrated in Figure 1 [1] [2]. Campaigns involve stealthy, persistent, and sophisticated activities, to establish a foothold in organizational systems, maintain that foothold and extend the set of resources the adversary controls, and exfiltrate sensitive information or disrupt operations.

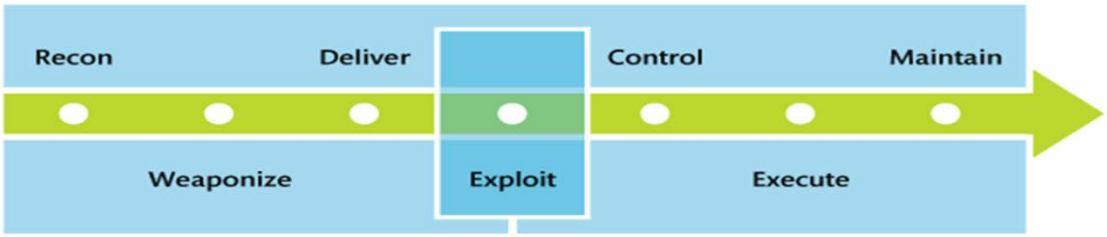

Figure 1. Cyber Attack Lifecycle

Organizations increasingly recognize that missions, business functions, systems, systems-of-systems, and mission segments need to be resilient in the face of the APT. Many organizations are adopting the multi-tier approach to risk management described in NIST Special Publication (SP) 800-39 [3], and the security lifecycle approach to risk management defined by the Risk Management Framework (RMF) in NIST SP 800-37 [4]. For those organizations, the question arises: How should security controls (or control enhancements) in NIST SP 800-53R4 [5] be selected, tailored, and implemented to improve cyber resiliency?[2]

This technical report identifies controls in NIST SP 800-53R4 that support cyber resiliency. The controls are characterized in terms of the resiliency techniques identified in MITRE's Cyber Resiliency Engineering Framework (CREF) [6]; Section 2 provides a brief overview of the CREF. Section 3 identifies factors to consider when selecting, tailoring, or implementing controls to improve cyber resiliency. The bulk of the document is in the Appendix, which identifies resiliency-related controls, provides the text of each control (or control enhancement), and maps the control or enhancement to the relevant cyber resiliency technique(s).

[1] The Cyber Attack Life Cycle, is a modification of what Lockheed Martin referred to as the "cyber kill chain" [13] [14].

[2] Information security risk management considers a wide range of possible threats, including environmental (e.g., natural disaster), structural (e.g., equipment failure), accidental, and adversarial [12]. Historically, descriptions of adversarial threats have focused on singular events by outsiders (e.g., intrusions, denial-of-service attacks), or on persistent abuses of access by insiders. The control baselines in NIST SP 800-53R4 address such adversarial threats, as well as environmental, structural, and accidental threats. However, as noted in Section 3.1 of NIST SP 800-53R4, the control baselines do not address the APT.

The rest of this introductory section discusses the characteristics of the APT that make this threat different from threats that have historically been the focus of information security risk management.

1.1 Distinguishing Characteristics of the APT

NIST SP 800-53 R4 [5] defines the APT as

> "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives."

Given the APT's expertise, resources, and persistence, even with correct implementation of all the necessary perimeter-based security, and continuous monitoring to ensure that patches are applied and vulnerabilities are closed, advanced adversaries will still breach the IT infrastructure [7]. Therefore, architecture and systems engineering must be based on the assumption that systems or components have been compromised (or contain undiscovered vulnerabilities that could lead to undetected compromises), and that missions and business functions must continue to operate in the presence of compromise. Therefore, today's systems need to be designed to be resilient against attacks by the APT.

It is important to understand that resiliency against the APT (henceforth referred to as cyber resiliency), while sharing many traits of traditional resiliency engineering (which generally focuses on resiliency against natural disasters and accidents), does have some key differences. Natural disasters are one-time events[3], or have predictable follow-on events (e.g., aftershocks and tsunamis for earthquakes). Moreover, natural disasters do not target specific structures or entities (although some, especially if not well constructed, may be more vulnerable to such events). Natural disasters do not evolve or change in response to activities by defenders to mitigate the event [7]. Nor do natural disasters take measures to hide or conceal themselves from detection, taking measures to better situate themselves for subsequent action. But the APT is able to do all these things. The need to deal with multi-pronged, targeted attacks that evolve and change in response to defender actions makes cyber resiliency different from the established resilience engineering discipline [7].

The challenge to resilience presented by the APT may be best considered via an analogy to healthcare [7]. People can exercise daily, eat balanced meals, get their required immunizations, and wash their hands frequently. But they still get infections, cancer, and heart attacks. That does not mean people should not do these proactive measures. Nor does it mean those measures are

[3] One notable exception is corrosion, which is a highly persistent threat. But while corrosion is a nature driven event, it is generally not thought of as a natural disaster.

not beneficial. It only means that they not sufficient. Hence, healthcare invested not only in preventative medications and techniques, but also in reactive medications and technique such as anti-cancer research/medication, post-heart-attack medication and treatment, etc. In some instances these reactive techniques can actually result in a cure. In other instances they contain or slow down the progress of the illness, with the focus of maximizing the patient's quality of life and longevity. The combination of proactive and reactive measures increases patients' overall resilience.

Similarly, cyber resiliency is not intended as a replacement for traditional cyber perimeter defense measures that are intended to keep the adversary out. Cyber resiliency is needed to complement these measures, both to make them more effective and so that when the adversary does breach the perimeter, the organization is able to maintain and maximize mission operations while containing and otherwise minimizing the spread and actions of the adversary.

2 MITRE's Cyber Resiliency Framework

As a vehicle for achieving consistent and structured discuss in the cyber resiliency space, MITRE has developed the cyber resilience engineering framework (CREF) [6]. The CREF, which is actually a partial ontology, draws from frameworks and taxonomies in the disciplines of resilience engineering [8] [9], network resilience [10], fault-tolerant and intrusion tolerant systems, and systems resilience in critical infrastructures[4]. While the CREF focuses on cyber, its derivation enables it to be extended (1) to extend the set of possible threat sources to include natural events and errors as well as adversarial actions; (2) to extend the set of adversarial actions to include non-cyber attack vectors; and (3) to consider cyber-physical as well as purely cyber systems.

As illustrated in Figure 2, the CREF consists of resiliency goals, objectives, and techniques.

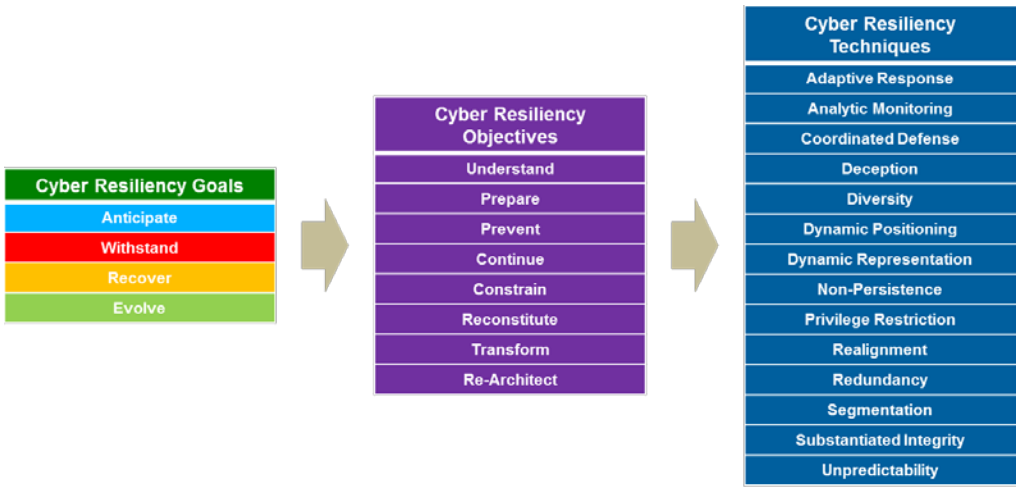

Figure 2. Cyber Resiliency Engineering Framework

Goals are high-level statements of intended outcomes. They help scope the cyber resiliency domain. The cyber resiliency goals defined in the CREF are identified and defined in Table 1.

Table 1. Cyber Resiliency Goals

Goal	Description
Anticipate	Maintain a state of informed preparedness in order to forestall compromises of mission function from potential adverse conditions
Withstand	Continue essential mission functions despite adverse conditions
Recover	Restore mission functions during and after the adverse conditions
Evolve	Change mission functions and/or supporting capabilities, so as to minimize adverse impacts from actual or predicted adverse conditions

[4] For more information on these frameworks and how the MITRE cyber resiliency engineering framework relates to them, see Appendix B of [6].

Objectives are more specific statements of intended outcomes, expressed so as to facilitate assessment; an objective can be identified with a single goal but may support achieving multiple goals. Objectives serve as a bridge between techniques and goals. They are expressed so as to facilitate assessment; it's straightforward to develop questions of "how well" or "how quickly" or "with what degree of confidence or trust" can each objective be achieved. They enable different stakeholders to assert their different priorities, based on mission. An objective can be identified with a single goal but may support achieving multiple goals. Table 2 defines the cyber resiliency objectives and also indicates (via color-coding) which goals they support and (via the size of the color-coded bar) the relative degree to which they support those goals.

Table 2. Cyber Resiliency Objectives

Objective	Description	Goals Supported
Understand	Maintain useful representations of mission dependencies and the status of resources with respect to possible adversity	
Prepare	Maintain a set of realistic courses of action that address predicted or anticipated adversity	
Prevent / Avoid	Preclude successful execution of attack or the realization of adverse conditions	
Continue	Maximize the duration and viability of essential mission functions during adverse conditions	
Constrain	Limit damage from adverse conditions	
Reconstitute	Redeploy resources to provide as compete a set of mission functionality as possible subsequent to adverse conditions	
Transform	Change aspects of organizational behavior in response to prior, current or prospective adverse conditions or attack	
Re-architect	Modify architectures for improved resilience	

Cyber resiliency techniques are ways to achieve one or more cyber resiliency objectives that are applied to the architecture or design of mission/business functions and the cyber resources that support them. Techniques are selectively[5] applied to the architecture or design of mission or business functions and the cyber resources that support them to achieve objectives; a given technique usually supports multiple objectives but may be unique to a single objective. The expectation is that the set of cyber resiliency techniques will change over time, as research in some of them fails to prove out, as others become standard cyber-security or COOP practice, and as new research ideas emerge. The cyber resiliency techniques in the CREF are identified and

[5] The importance of selectivity cannot be overstated: implementations of some techniques will interfere with or render infeasible implementations of others; technologies vary in maturity and scalability. Therefore, political, operational, economic, and technical factors must be taken into consideration in selecting and applying cyber resiliency techniques to an architecture.

defined in Table 3. Table 4 provides a mapping between the cyber resiliency objectives and techniques in the CREF.

Table 3. Cyber Resiliency Techniques

Technique	Description
Adaptive Response	Respond appropriately and dynamically to specific situations, using agile and alternative operational contingencies to maintain minimum operational capabilities, in order to limit consequences and avoid destabilization, taking preemptive action where appropriate
Analytic Monitoring	Continuously gather, fuse, and analyze data to use threat intelligence, identify vulnerabilities, find indications of potential adverse conditions, and identify potential or actual damage
Coordinated Defense	Coordinate multiple, distinct mechanisms (defense-in-depth) to protect critical resources, across subsystems, layers, systems, and organizations
Deception	Confuse, deceive and mislead the adversary
Diversity	Use a heterogeneous set of technologies, data sources, processing locations, and communications paths to minimize common mode failures (including attacks exploiting common vulnerabilities)
Dynamic Positioning	Distribute and dynamically relocate functionality and assets
Dynamic Representation	Support mission situation awareness and response by using dynamic representations of components, systems, services, adversary activities and other adverse situations, and effects of alternative courses of action
Non-Persistence	Retain information, services, and connectivity for a limited time, thereby reducing exposure to corruption, modification, or usurpation
Privilege Restriction	Design to restrict privileges assigned to users and cyber entities, and to set privilege requirements on resources based on criticality
Realignment	Enable resources to be aligned (or realigned) with core mission functions, thus reducing the attack surface, the potential for unintended consequences, and the potential for cascading failures
Redundancy	Provide multiple protected instances of critical information and resources, to reduce the consequences of loss
Segmentation / Separation	Separate (logically or physically) components based on criticality and trustworthiness, to limit the spread of damage
Substantiated Integrity	Provide mechanisms to ascertain whether critical services, information stores, information streams, and components have been corrupted
Unpredictability	Make changes, frequently and randomly, to make the attack surface unpredictable

Table 4. Mapping Cyber Resiliency Techniques to Objectives

	Understand	Prepare	Prevent	Constrain	Continue	Reconstitute	Transform	Re-Architect
Adaptive Response				X	X	X		
Analytic Monitoring	X	X		X		X		
Coordinated Defense		X	X	X	X	X		
Deception	X		X		X			
Diversity			X		X			X
Dynamic Positioning	X		X		X			X
Dynamic Representation	X	X					X	
Non-Persistence			X	X	X			X
Privilege Restriction			X	X				
Realignment				X			X	
Redundancy					X	X		
Segmentation			X	X				
Substantiated Integrity	X			X	X	X		
Unpredictability	X		X		X			

The framework of cyber resiliency goals, objectives, and techniques is intended to map the cyber resiliency solution space. Overlapping regions on a map (e.g., states and watersheds on a geographical map) are to be expected. In addition, the geography continues to change, as threats evolve and new resilience-related technologies transition from research to operational use.

The CREF is deliberately incomplete: Objectives and techniques that relate to organizational resilience or business continuity in the face of non-cyber threats (e.g., natural disaster, human error) are not included. The CREF assumes a good foundation of cyber-security and continuity of operations (COOP), as described in the security control baselines in NIST SP 800-53R4.

This section has provided an overview of the CREF. For more details, see [6] and [11].

3 Selecting NIST SP 800-53R4 Controls that Support Cyber Resiliency Techniques

As discussed above, cyber resiliency is a topic of growing interest and concern across the community. The level of abstraction in the MITRE CREF is intended to facilitate analysis at a relatively high level of abstraction, and aid senior decision makers in determining where they wish to place their emphasis. That means that the elements of the CREF, even the CREF techniques and the more specific capabilities and approaches they use[6], are at too high a level to directly support the system security engineer in identifying and allocating capabilities to elements (e.g., common infrastructure, shared service, subsystem or component, system in a system-of-systems) in an architecture or design. Possible capabilities, to support system security engineering analysis, are better expressed as controls in NIST SP 800-53R4 [5].

NIST SP 800-53R4 has over 860 control and enhancements. Not surprisingly, the majority of controls in NIST 800-53R4 are not resiliency oriented. Rather the bulk of the controls are oriented to achieving the information system security goals of confidentiality, integrity, and availability. Still, approximately 17% of the controls[7] in NIST 800-53R4 are cyber resiliency oriented. But because of the sheer number of controls it is not easy to identify which controls support resiliency and for those that do support resiliency, what aspect of resiliency do they support. Such identification is needed for those developing system requirements as well as resiliency overlays. Appendix A provides this identification.

Rather than simply tag controls as being resiliency-oriented, Appendix A categorizes the resiliency-oriented controls with regards to what aspect of resiliency they support. This is done by mapping the controls against the 14 cyber resiliency techniques defined in [6]. As with any taxonomy and mapping, the information in Appendix A is of course open to interpretation.

Readers are strongly cautioned ***not*** to view the contents of the table as a set of controls that must all be implemented to achieve resiliency. There are a variety of factors an organization needs to consider in selecting the appropriate resiliency supporting controls. These include

- **Organizational goals and objectives**: Different stakeholders are likely to have different goals and objectives. Mission commanders are concerned by the need to ensure that the mission is carried out to fullest extent. Thus, they may be most interested in the goals of Anticipate and Withstand and the objectives and techniques and controls that support those goals. In contrast, cyber-defenders are likely to be concerned with the ability to respond quickly to cyber-attacks in their operational environment.
- **Maturity of techniques and controls:** Some techniques (and supporting controls) are more mature than others. For some stakeholders the relative maturity of a given technique is important in determining whether or not to invest in and select it. See Appendices D and F of [11] for more on the relative maturity of techniques.

[6] See Appendix D of [11].
[7] The term "controls" is used in this document to refer to both controls and control enhancements (CEs) in NIST SP 800-53.

- **Operational application in current practice**: Some techniques (and supporting controls) are more commonly used in practice today than others. Many organizations may opt to select techniques that are more commonly used, as they will equate (sometime mistakenly) common practice for best practice.
- **Political, Operational, Economic, Technical (POET) considerations**: Various POET considerations can greatly impact whether an organization might select a given cyber resiliency technique and control. For example, environments with very limited processing capability (e.g., embedded systems) would likely not find techniques such as deception nets very useful. See Appendix E of [11] for more information on POET considerations for cyber resiliency techniques.
- **Nature of the adversary**: An adversarial threat can be assessed with regards to its capability, intent and targeting. (See Appendix D of NIST SP 800-30 R1 [12].) This can have a direct bearing on the determination of which resiliency techniques are likely to be most appropriate with regards to countering the adversary. For example, an adversary that has the capability of developing and deploying new zero-day attacks tailored to the systems that the defender is known to employ might best be addressed by the defender employing techniques such as deception (e.g., SC-36 Honeypots) to discern the nature of the attack techniques and diversity (e.g., use of different systems, services, or applications at key locations) to impede the adversary's ability to successfully target the organization's systems.

Based on an organization's assessment of these factors it would determine which of the identified cyber resiliency controls is more appropriate for their needs. These factors could also be used to help in the development of one (or more) cyber resiliency overlays.

Appendix A Mapping Resiliency Techniques to NIST SP 800-53 R4 Controls

The table below reflects the author's view of which NIST 800-53R4 controls and control enhancements (CEs) support which CREF techniques. In several cases a control supports multiple techniques[8].

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
1.	AC-2 (6)	*ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT*	The information system implements the following dynamic privilege management capabilities: [*Assignment: organization-defined list of dynamic privilege management capabilities*].	Privilege Restriction and Adaptive Response
2.	AC-3 (2)	*ACCESS ENFORCEMENT | DUAL AUTHORIZATION*	The information system enforces dual authorization for [*Assignment: organization-defined privileged commands and/or other organization-defined actions*].	Privilege Restriction
3.	AC-3 (9)	*ACCESS ENFORCEMENT | CONTROLLED RELEASE*	The information system does not release information outside of the established system boundary unless: (a) The receiving [*Assignment: organization-defined information system or system component*] provides [*Assignment: organization-defined security safeguards*]; and (b) [*Assignment: organization-defined security safeguards*] are used.	Privilege Restriction
4.	AC-4 (2)	*INFORMATION FLOW ENFORCEMENT | PROCESSING DOMAINS*	The information system uses protected processing domains to enforce *[Assignment: organization-defined information flow control policies]* as a basis for flow control decisions.	Segmentation
5.	AC-4 (3)	*INFORMATION FLOW ENFORCEMENT | DYNAMIC INFORMATION FLOW CONTROL*	The information system enforces dynamic information flow control based on *[Assignment: organization-defined policies]*.	Adaptive Response

[8] If more than one resiliency technique is identified, but the techniques are not joined by "and", the control implements some aspect of each technique. If techniques are joined by "and", the control implements a synergistic combination of the techniques.

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
6.	AC-4 (8)	*INFORMATION FLOW ENFORCEMENT | SECURITY POLICY FILTERS*	The information system enforces information flow control using *[Assignment: organization-defined security policy filters]* as a basis for flow control decisions for *[Assignment: organization-defined information flows]*.	Substantiated Integrity
7.	AC-4 (21)	*INFORMATION FLOW ENFORCEMENT | PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS*	The information system separates information flows logically or physically using [*Assignment: organization-defined mechanisms and/or techniques*] to accomplish [*Assignment: organization-defined required separations by types of information*].	Segmentation
8.	AC-6	LEAST PRIVILEGE	Control: The organization: a. Separates [*Assignment: organization-defined duties of individuals*]; b. Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties.	Privilege Restriction
9.	AC-6 (1)	*LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*	The organization explicitly authorizes access to [*Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information*].	Privilege Restriction
10.	AC-6 (2)	*LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*	The organization requires that users of information system accounts, or roles, with access to [*Assignment: organization-defined security functions or security-relevant information*], use non-privileged accounts or roles, when accessing nonsecurity functions.	Privilege Restriction
11.	AC-6 (3)	*LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS*	The organization authorizes network access to [*Assignment: organization-defined privileged commands*] only for [*Assignment: organization-defined compelling operational needs*] and documents the rationale for such access in the security plan for the information system.	Privilege Restriction

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
12.	AC-6 (4)	*LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS*	The information system provides separate processing domains to enable finer-grained allocation of user privileges.	Privilege Restriction
13.	AC-6 (5)	*LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*	The organization restricts privileged accounts on the information system to [*Assignment: organization-defined personnel or roles*].	Privilege Restriction
14.	AC-6 (6)	*LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS*	The organization prohibits privileged access to the information system by non-organizational users.	Privilege Restriction
15.	AC-6 (7)	*LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES*	The organization: (a) Reviews [*Assignment: organization-defined frequency*] the privileges assigned to [*Assignment: organization-defined roles or classes of users*] to validate the need for such privileges; and (b) Reassigns or removes privileges,	Privilege Restriction
16.	AC-6 (8)	*LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION*	The information system prevents [*Assignment: organization-defined software*] from executing at higher privilege levels than users executing the software.	Privilege Restriction
17.	AC-6 (10)	*LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*	The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	Privilege Restriction
18.	AT-3 (3)	*SECURITY TRAINING | PRACTICAL EXERCISES*	The organization includes practical exercises in security training that reinforce training objectives.	Coordinated Defense
19.	AU-6 (5)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | INTEGRATION / SCANNING AND MONITORING CAPABILITIES*	The organization integrates analysis of audit records with analysis of [*Selection (one or more): vulnerability scanning information; performance data; information system monitoring information;* [*Assignment: organization-defined data/information collected from other sources*]] to further enhance the ability to identify inappropriate or unusual activity.	Analytic Monitoring

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
20.	AU-6 (6)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING*	The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.	Analytic Monitoring
21.	AU-6 (8)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS*	The organization performs a full text analysis of audited privileged commands in a physically distinct component or subsystem of the information system, or other information system that is dedicated to that analysis.	Privilege Restriction Analytic Monitoring Segmentation
22.	AU-9 (2)	*PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS*	The information system backs up audit records [*Assignment: organization-defined frequency*] onto a physically different system or system component than the system or component being audited.	Segmentation Redundancy
23.	AU-9 (5)	*PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION*	The organization enforces dual authorization for [*Selection (one or more): movement; deletion*] of [*Assignment: organization-defined audit information*].	Privilege Restriction
24.	AU-15	ALTERNATE AUDIT CAPABILITY	The organization provides an alternate audit capability in the event of a failure in primary audit capability that provides [*Assignment: organization-defined alternate audit functionality*].	Redundancy
25.	CA-3 (1)	*SYSTEM INTERCONNECTIONS | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS*	The organization prohibits the direct connection of an [*Assignment: organization-defined unclassified, national security system*] to an external network without the use of [*Assignment: organization-defined boundary protection device*].	Segmentation
26.	CA-3 (2)	*SYSTEM INTERCONNECTIONS | CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS*	The organization prohibits the direct connection of a classified, national security system to an external network without the use of [*Assignment: organization-defined boundary protection device*].	Segmentation

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
27.	CA-3 (3)	*SYSTEM INTERCONNECTIONS | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS*	The organization prohibits the direct connection of an [*Assignment: organization-defined unclassified, non-national security system*] to an external network without the use of [*Assignment; organization-defined boundary protection device*].	Segmentation
28.	CA-3 (4)	*SYSTEM INTERCONNECTIONS | CONNECTIONS TO PUBLIC NETWORKS*	The organization prohibits the direct connection of an [*Assignment: organization-defined information system*] to a public network.	Segmentation
29.	CA-8	PENETRATION TESTING	The organization conducts penetration testing [*Assignment: organization-defined frequency*] on [*Assignment: organization-defined information systems or system components*].	Analytic Monitoring
30.	CM-5 (4)	*ACCESS RESTRICTIONS FOR CHANGE | DUAL-AUTHORIZATION*	The organization enforces dual authorization for implementing changes to [*Assignment: organization-defined information system components and system-level information*].	Privilege Restriction
31.	CM-5 (5)	*ACCESS RESTRICTIONS FOR CHANGE | LIMIT PRODUCTION / OPERATIONAL PRIVILEGES*	The organization: (a) Limits privileges to change information system components and system-related information within a production or operational environment; and (b) Reviews and reevaluates privileges [*Assignment: organization-defined frequency*].	Privilege Restriction
32.	CM-5 (6)	*ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES*	The organization limits privileges to change software resident within software libraries.	Privilege Restriction

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
33.	CM-7 (1)	*LEAST FUNCTIONALITY | PERIODIC REVIEW*	The organization: (a) Reviews the information system [*Assignment: organization-defined frequency*] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and (b) Disables [*Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure*].	Privilege Restriction
34.	CM-11 (1)	*USER-INSTALLED SOFTWARE | ALERTS FOR UNAUTHORIZED INSTALLATIONS*	The information system alerts [*Assignment: organization-defined personnel or roles*] when the unauthorized installation of software is detected.	Privilege Restriction
35.	CP-2 (5)	*CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*	The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.	Coordinated Defense and Dynamic Representation
36.	CP-2 (8)	*CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*	The organization identifies critical information system assets supporting essential missions and business functions.	Dynamic Representation
37.	CP-6	ALTERNATE STORAGE SITE	The organization: a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site	Redundancy
38.	CP-6 (1)	*ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*	The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.	Redundancy

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
39.	CP-7	ALTERNATE PROCESSING SITE	The organization: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [*Assignment: organization-defined information system operations*] for essential missions/business functions within [*Assignment: organization-defined time period consistent with recovery time and recovery point objectives*] when the primary processing capabilities are unavailable; b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.	Redundancy
40.	CP-7 (1)	*ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE*	The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.	Redundancy
41.	CP-8	TELECOMMUNICATIONS SERVICES	The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	Redundancy and Diversity
42.	CP-8 (3)	*TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS*	The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.	Redundancy

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
43.	CP-9	INFORMATION SYSTEM BACKUP	The organization: a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; b. Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; c. Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and d. Protects the confidentiality, integrity, and availability of backup information at storage locations.	Redundancy
44.	CP-9 (6)	*INFORMATION SYSTEM BACKUP | REDUNDANT SECONDARY SYSTEM*	The organization accomplishes information system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.	Redundancy
45.	CP-9 (7)	*INFORMATION SYSTEM BACKUP | DUAL AUTHORIZATION*	The organization enforces dual authorization for the deletion or destruction of [*Assignment: organization-defined backup information*]. Supplemental Guidance: Dual authorization	Privilege Restriction
46.	CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	Adaptive Response Coordinated Defense Substantiated Integrity

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
47.	CP-11	ALTERNATE COMMUNICATIONS PROTOCOLS	The information system provides the capability to employ [*Assignment: organization-defined alternative communications protocols*] in support of maintaining continuity of operations.	Diversity
48.	CP-13	ALTERNATIVE SECURITY MECHANISMS	The organization employs [*Assignment: organization-defined alternative or supplemental security mechanisms*] for satisfying [*Assignment: organization-defined security functions*] when the primary means of implementing the security function is unavailable or compromised.	Redundancy Diversity Adaptive Response
49.	IA-2 (6)	*IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - SEPARATE DEVICE*	The information system implements multifactor authentication for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*Assignment: organization-defined strength of mechanism requirements*].	Coordinated Defense
50.	IA-2 (7)	*IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - SEPARATE DEVICE*	The information system implements multifactor authentication for network access to non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*Assignment: organization-defined strength of mechanism requirements*].	Coordinated Defense
51.	IA-2 (11)	*IDENTIFICATION AND AUTHENTICATION | REMOTE ACCESS - SEPARATE DEVICE*	The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*Assignment: organization-defined strength of mechanism requirements*].	Coordinated Defense
52.	IA-2 (13)	*IDENTIFICATION AND AUTHENTICATION | OUT-OF-BAND AUTHENTICATION*	The information system implements [*Assignment: organization-defined out-of-band authentication*] under [*Assignment: organization-defined conditions*].	Coordinated Defense Redundancy and Diversity

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
53.	IA-10	ADAPTIVE IDENTIFICATION AND AUTHENTICATION	The organization requires that individuals accessing the information system employ [*Assignment: organization-defined supplemental authentication techniques or mechanisms*] under specific [*Assignment: organization-defined circumstances or situations*].	Diversity Adaptive Response
54.	IR-4 (2)	*INCIDENT HANDLING | DYNAMIC RECONFIGURATION*	The organization includes dynamic reconfiguration of [*Assignment: organization-defined information system components*] as part of the incident response capability.	Adaptive Response
55.	IR-4 (3)	*INCIDENT HANDLING | CONTINUITY OF OPERATIONS*	The organization identifies [*Assignment: organization-defined classes of incidents*] and [*Assignment: organization-defined actions to take in response to classes of incidents*] to ensure continuation of organizational missions and business functions.	Adaptive Response Coordinated Defense
56.	IR-4 (4)	*INCIDENT HANDLING | INFORMATION CORRELATION*	The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	Adaptive Response, Coordinated Defense and Analytic Monitoring
57.	IR-4 (9)	*INCIDENT HANDLING | DYNAMIC RESPONSE CAPABILITY*	The organization employs [*Assignment: organization-defined dynamic response capabilities*] to effectively respond to security incidents.	Adaptive Response
58.	IR-4 (10)	*INCIDENT HANDLING | SUPPLY CHAIN COORDINATION*	The organization coordinates incident handling activities involving supply chain events with other organizations involved in the supply chain.	Coordinated Defense
59.	IR-10	INTEGRATED INFORMATION SECURITY ANALYSIS TEAM	The organization establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.	Adaptive Response and Analytic Monitoring

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
60.	MA-4 (4)	*NONLOCAL MAINTENANCE | AUTHENTICATION / SEPARATION OF MAINTENANCE SESSIONS*	The organization protects nonlocal maintenance sessions by: (a) Employing [*Assignment: organization-defined authenticators that are replay resistant*]; and (b) Separating the maintenance sessions from other network sessions with the information system by either: (1) Physically separated communications paths; or (2) Logically separated communications paths based upon encryption.	Segmentation
61.	PE-3 (2)	*PHYSICAL ACCESS CONTROL | FACILITY / INFORMATION SYSTEM BOUNDARIES*	The organization performs security checks [*Assignment: organization-defined frequency*] at the physical boundary of the facility or information system for unauthorized exfiltration of information or removal of information system components.	Analytic Monitoring
62.	PE-3 (4)	*PHYSICAL ACCESS CONTROL | LOCKABLE CASINGS*	The organization uses lockable physical casings to protect [*Assignment: organization-defined information system components*] from unauthorized physical access.	Coordinated Defense
63.	PE-3 (5)	*PHYSICAL ACCESS CONTROL | TAMPER PROTECTION*	The organization employs [*Assignment: organization-defined security safeguards*] to [*Selection (one or more): detect; prevent*] physical tampering or alteration of [*Assignment: organization-defined hardware components*] within the information system.	Substantiated Integrity
64.	PE-3 (6)	*PHYSICAL ACCESS CONTROL | FACILITY PENETRATION TESTING*	The organization employs a penetration testing process that includes [*Assignment: organization-defined frequency*], unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.	Analytic Monitoring

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
65.	PE-6	MONITORING PHYSICAL ACCESS	The organization: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs [*Assignment: organization-defined frequency*] and upon occurrence of [*Assignment: organization-defined events or potential indications of events*]; and c. Coordinates results of reviews and investigations with the organizational incident response capability.	Analytic Monitoring
66.	PE-6 (2)	*MONITORING PHYSICAL ACCESS | AUTOMATED INTRUSION RECOGNITION / RESPONSES*	The organization employs automated mechanisms to recognize [*Assignment: organization-defined classes/types of intrusions*] and initiate [*Assignment: organization-defined response actions*].	Analytic Monitoring and Adaptive Response
67.	PE-6 (4)	*MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS*	The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as [*Assignment: organization-defined physical spaces containing one or more components of the information system*].	Analytic Monitoring and Coordinated Defense
68.	PE-9 (1)	*POWER EQUIPMENT AND CABLING | REDUNDANT CABLING*	The organization employs redundant power cabling paths that are physically separated by [*Assignment: organization-defined distance*].	Redundancy
69.	PE-11 (1)	*EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY*	The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.	Redundancy

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
70.	PE-11 (2)	*EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - SELF-CONTAINED*	The organization provides a long-term alternate power supply for the information system that is: (a) Self-contained; (b) Not reliant on external power generation; and (c) Capable of maintaining [*Selection: minimally required operational capability; full operational capability*] in the event of an extended loss of the primary power source.	Redundancy
71.	PE-17	ALTERNATE WORK SITE	The organization: a. Employs [*Assignment: organization-defined security controls*] at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.	Redundancy
72.	PL-2 (3)	*SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES*	The organization plans and coordinates security-related activities affecting the information system with [*Assignment: organization-defined individuals or groups*] before conducting such activities in order to reduce the impact on other organizational entities.	Coordinated Defense
73.	PL-8 (1)	*INFORMATION SECURITY ARCHITECTURE | DEFENSE-IN-DEPTH*	The organization designs its security architecture using a defense-in-depth approach that: (a) Allocates [*Assignment: organization-defined security safeguards*] to [*Assignment: organization-defined locations and architectural layers*]; and (b) Ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.	Coordinated Defense

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
74.	PL-8 (2)	*INFORMATION SECURITY ARCHITECTURE | SUPPLIER DIVERSITY*	The organization requires that [*Assignment: organization-defined security safeguards*] allocated to [*Assignment: organization-defined locations and architectural layers*] are obtained from different suppliers.	Diversity
75.	RA-5 (5)	*VULNERABILITY SCANNING | PRIVILEGED ACCESS*	The information system implements privileged access authorization to [*Assignment: organization-identified information system components*] for selected [*Assignment: organization-defined vulnerability scanning activities*].	Analytic Monitoring Privilege Restriction
76.	RA-5 (6)	*VULNERABILITY SCANNING | AUTOMATED TREND ANALYSES*	The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.	Analytic Monitoring
77.	RA-5 (8)	*VULNERABILITY SCANNING | REVIEW HISTORIC AUDIT LOGS*	The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.	Analytic Monitoring
78.	RA-5 (10)	*VULNERABILITY SCANNING | CORRELATE SCANNING INFORMATION*	The organization correlates the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.	Analytic Monitoring
79.	SA-12	SUPPLY CHAIN PROTECTION	The organization protects against supply chain threats to the information system, system component, or information system service by employing [*Assignment: organization-defined security safeguards*] as part of a comprehensive, defense-in-breadth information security strategy.	Substantiated Integrity
80.	SA-12 (1)	*SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS*	The organization employs [*Assignment: organization-defined tailored acquisition strategies, contract tools, and procurement methods*] for the purchase of the information system, system component, or information system service from suppliers.	Substantiated Integrity and Redundancy

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
81.	SA-12 (5)	*SUPPLY CHAIN PROTECTION | LIMITATION OF HARM*	The organization employs [*Assignment: organization-defined security safeguards*] to limit harm from potential adversaries identifying and targeting the organizational supply chain.	Diversity and Deception
82.	SA-12 (10)	*SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT ALTERED*	The organization employs [*Assignment: organization-defined security safeguards*] to validate that the information system or system component received is genuine and has not been altered.	Substantiated Integrity
83.	SA-12 (11)	*SUPPLY CHAIN PROTECTION | PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS*	The organization employs [*Selection (one or more): organizational analysis, independent third-party analysis, organizational penetration testing, independent third-party penetration testing*] of [*Assignment: organization-defined supply chain elements, processes, and actors*] associated with the *information system, system component, or information system service*.	Analytic Monitoring Substantiated Integrity
84.	SA-12 (13)	*SUPPLY CHAIN PROTECTION | CRITICAL INFORMATION SYSTEM COMPONENTS*	The organization employs [*Assignment: organization-defined security safeguards*] to ensure an adequate supply of [*Assignment: organization-defined critical information system components*].	Redundancy Diversity
85.	SA-12 (14)	*SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY*	The organization establishes and retains unique identification of [*Assignment: organization-defined supply chain elements, processes, and actors*] for the information system, system component, or information system service.	Analytic Monitoring Dynamic Representation

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
86.	SA-14	CRITICALITY ANALYSIS	The organization identifies critical information system components and functions by performing a criticality analysis for [*Assignment: organization-defined information systems, information system components, or information system services*] at [*Assignment: organization-defined decision points in the system development life cycle*].	Dynamic Representation Realignment
87.	SA-15 (5)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION*	The organization requires the developer of the information system, system component, or information system service to reduce attack surfaces to [*Assignment: organization-defined thresholds*].	Realignment, Privilege Restriction, and Coordinated Defense
88.	SA-17 (7)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR LEAST PRIVILEGE*	The organization requires the developer of the information system, system component, or information system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.	Privilege Restriction
89.	SA-18	TAMPER RESISTANCE AND DETECTION	The organization implements a tamper protection program for the information system, system component, or information system service.	Substantiated Integrity
90.	SA-18 (1)	*TAMPER RESISTANCE AND DETECTION | MULTIPLE PHASES OF SDLC*	The organization employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including design, development, integration, operations, and maintenance.	Substantiated Integrity
91.	SA-18 (2)	*TAMPER RESISTANCE AND DETECTION | INSPECTION OF INFORMATION SYSTEMS, COMPONENTS, OR DEVICES*	The organization inspects [*Assignment: organization-defined information systems, system components, or devices*] [*Selection (one or more): at random;* at [*Assignment: organization-defined frequency*], *upon* [*Assignment: organization-defined indications of need for inspection*]] to detect tampering.	Substantiated Integrity

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
92.	SA-19	COMPONENT AUTHENTICITY	The organization: a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the information system; and b. Reports counterfeit information system components to [*Selection (one or more): source of counterfeit component;* [*Assignment: organization-defined external reporting organizations*]; [*Assignment: organization-defined personnel or roles*]].	Substantiated Integrity
93.	SA-20	CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS	The organization re-implements or custom develops [*Assignment: organization-defined critical information system components*].	Diversity
94.	SC-3	SECURITY FUNCTION ISOLATION	The information system isolates security functions from nonsecurity functions	Segmentation
95.	SC-3 (3)	*SECURITY FUNCTION ISOLATION | MINIMIZE NONSECURITY FUNCTIONALITY*	The organization minimizes the number of nonsecurity functions included within the isolation boundary containing security functions.	Segmentation Realignment
96.	SC-7 (10)	*BOUNDARY PROTECTION | UNAUTHORIZED EXFILTRATION*	The organization prevents the unauthorized exfiltration of information across managed interfaces.	Analytic Monitoring and Realignment
97.	SC-7 (11)	*BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC*	The information system only allows incoming communications from [*Assignment: organization-defined authorized sources*] routed to [*Assignment: organization-defined authorized destinations*].	Realignment Segmentation
98.	SC-7 (13)	*BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS*	The organization isolates [*Assignment: organization-defined information security tools, mechanisms, and support components*] from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.	Segmentation

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
99.	SC-7 (15)	*BOUNDARY PROTECTION | ROUTE PRIVILEGED NETWORK ACCESSES*	The information system routes all networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.	Realignment Segmentation Privilege Restriction
100.	SC-7 (20)	*BOUNDARY PROTECTION | DYNAMIC ISOLATION / SEGREGATION*	The information system provides the capability to dynamically isolate/segregate [*Assignment: organization-defined information system components*] from other components of the system.	Segmentation and Adaptive Response
101.	SC-7 (21)	*BOUNDARY PROTECTION | ISOLATION OF INFORMATION SYSTEM COMPONENTS*	The organization employs boundary protection mechanisms to separate [*Assignment: organization-defined information system components*] supporting [*Assignment: organization-defined missions and/or business functions*].	Segmentation
102.	SC-7 (22)	*BOUNDARY PROTECTION | SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS*	The information system implements separate network addresses (i.e., different subnets) to connect to systems in different security domains.	Segmentation
103.	SC-8 (4)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL / RANDOMIZE COMMUNICATIONS*	The information system implements cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by [*Assignment: organization-defined alternative physical safeguards*].	Deception and Unpredictability
104.	SC-23 (3)	*SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION*	The information system generates a unique session identifier for each session with [*Assignment: organization-defined randomness requirements*] and recognizes only session identifiers that are system-generated.	Unpredictability
105.	SC-25	THIN NODES	The organization employs [*Assignment: organization-defined information system components*] with minimal functionality and information storage.	Privilege Restriction

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
106.	SC-26	HONEYPOTS	The information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.	Deception
107.	SC-27	PLATFORM-INDEPENDENT APPLICATIONS	The information system includes: [*Assignment: organization-defined platform-independent applications*].	Diversity and Dynamic Positioning
108.	SC-29	HETEROGENEITY	The organization employs a diverse set of information technologies for [*Assignment: organization-defined information system components*] in the implementation of the information system.	Diversity
109.	SC-29 (1)	*HETEROGENEITY | VIRTUALIZATION TECHNIQUES*	The organization employs virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [*Assignment: organization-defined frequency*].	Diversity
110.	SC-30	CONCEALMENT AND MISDIRECTION	The organization employs [*Assignment: organization-defined concealment and misdirection techniques*] for [*Assignment: organization-defined information systems*] at [*Assignment: organization-defined time periods*] to confuse and mislead adversaries.	Deception
111.	SC-30 (2)	*CONCEALMENT AND MISDIRECTION | RANDOMNESS*	The organization employs [*Assignment: organization-defined techniques*] to introduce randomness into organizational operations and assets.	Unpredictability
112.	SC-30 (3)	*CONCEALMENT AND MISDIRECTION | CHANGE PROCESSING / STORAGE LOCATIONS*	The organization changes the location of [*Assignment: organization-defined processing and/or storage*] [*Selection:* [*Assignment: organization-defined time frequency*]*; at random time intervals*]].	Dynamic Positioning and Unpredictability
113.	SC-30 (4)	*CONCEALMENT AND MISDIRECTION | MISLEADING INFORMATION*	The organization employs realistic, but misleading information in [*Assignment: organization-defined information system components*] with regard to its security state or posture.	Deception

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
114.	SC-30 (5)	*CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM COMPONENTS*	The organization employs [*Assignment: organization-defined techniques*] to hide or conceal [*Assignment: organization-defined information system components*].	Deception
115.	SC-32	INFORMATION SYSTEM PARTITIONING	The organization partitions the information system into [*Assignment: organization-defined information system components*] residing in separate physical domains or environments based on [*Assignment: organization-defined circumstances for physical separation of components*].	Segmentation
116.	SC-34	NON-MODIFIABLE EXECUTABLE PROGRAMS	The information system at [*Assignment: organization-defined information system components*]: a. Loads and executes the operating environment from hardware-enforced, read-only media; and b. Loads and executes [*Assignment: organization-defined applications*] from hardware-enforced, read-only media.	Substantiated Integrity
117.	SC-34 (1)	*NON-MODIFIABLE EXECUTABLE PROGRAMS | NO WRITABLE STORAGE*	The organization employs [*Assignment: organization-defined information system components*] with no writeable storage that is persistent across component restart or power on/off.	Non-Persistence
118.	SC-34 (2)	*NON-MODIFIABLE EXECUTABLE PROGRAMS | INTEGRITY PROTECTION / READ-ONLY MEDIA*	The organization protects the integrity of information prior to storage on read-only media and controls the media after such information has been recorded onto the media.	Substantiated Integrity

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
119.	SC-34 (3)	*NON-MODIFIABLE EXECUTABLE PROGRAMS | HARDWARE-BASED PROTECTION*	The organization: (a) Employs hardware-based, write-protect for [*Assignment: organization-defined information system firmware components*]; and (b) Implements specific procedures for [*Assignment: organization-defined authorized individuals*] to manually disable hardware write-protect for firmware modifications and re-enable the write-protect prior to returning to operational mode.	Substantiated Integrity
120.	SC-35	HONEYCLIENTS	The information system includes components that proactively seek to identify malicious websites and/or web-based malicious code.	Deception
121.	SC-36	DISTRIBUTED PROCESSING AND STORAGE	The organization distributes [*Assignment: organization-defined processing and storage*] across multiple physical locations.	Dynamic Positioning and Redundancy
122.	SC-36 (1)	*DISTRIBUTED PROCESSING AND STORAGE | POLLING TECHNIQUES*	The organization employs polling techniques to identify potential faults, errors, or compromises to [*Assignment: organization-defined distributed processing and storage components*].	Substantiated Integrity
123.	SC-37	OUT-OF-BAND CHANNELS	The organization employs [*Assignment: organization-defined out-of-band channels*] for the physical delivery or electronic transmission of [*Assignment: organization-defined information, information system components, or devices*] to [*Assignment: organization-defined individuals or information systems*].	Diversity
124.	SC-39	PROCESS ISOLATION	The information system maintains a separate execution domain for each executing process.	Segmentation
125.	SC-44	DETONATION CHAMBERS	The organization employs a detonation chamber capability within [*Assignment: organization-defined information system, system component, or location*].	Deception

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
126.	SI-3 (10)	*MALICIOUS CODE PROTECTION | MALICIOUS CODE ANALYSIS*	The organization: a. Employs [*Assignment: organization-defined tools and techniques*] to analyze the behavior of malware; and b. Incorporates the results from malware analysis into organizational incident response and flaw remediation processes.	Analytic Monitoring
127.	SI-4 (3)	*INFORMATION SYSTEM MONITORING | AUTOMATED TOOL INTEGRATION*	The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.	Analytic Monitoring and Adaptive Response
128.	SI-4 (10)	*INFORMATION SYSTEM MONITORING | VISIBILITY OF ENCRYPTED COMMUNICATIONS*	The organization makes provisions so that [*Assignment: organization-defined encrypted communications traffic*] is visible to [*Assignment: organization-defined information system monitoring tools*].	Analytic Monitoring
129.	SI-4 (11)	*INFORMATION SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES*	The organization analyzes outbound communications traffic at the external boundary of the information system and selected [*Assignment: organization-defined interior points within the system (e.g., subnetworks, subsystems)*] to discover anomalies.	Analytic Monitoring
130.	SI-4 (16)	*INFORMATION SYSTEM MONITORING | CORRELATE MONITORING INFORMATION*	The organization correlates information from monitoring tools employed throughout the information system.	Analytic Monitoring and Dynamic Representation
131.	SI-4 (17)	*INFORMATION SYSTEM MONITORING | INTEGRATED SITUATIONAL AWARENESS*	The organization correlates information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.	Dynamic Representation

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
132.	SI-4 (18)	*INFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / COVERT EXFILTRATION*	The organization analyzes outbound communications traffic at the external boundary of the information system (i.e., system perimeter) and at [*Assignment: organization-defined interior points within the system (e.g., subsystems, subnetworks)*] to detect covert exfiltration of information.	Analytic Monitoring
133.	SI-4 (20)	*INFORMATION SYSTEM MONITORING | PRIVILEGED USER*	The organization implements [*Assignment: organization-defined additional monitoring*] of privileged users.	Analytic Monitoring Privilege Restriction
134.	SI-4 (24)	*INFORMATION SYSTEM MONITORING | INDICATORS OF COMPROMISE*	The information system discovers, collects, distributes, and uses indicators of compromise.	Analytic Monitoring
135.	SI-6	SECURITY FUNCTION VERIFICATION	The information system: a. Verifies the correct operation of [*Assignment: organization-defined security functions*]; b. Performs this verification [*Selection (one or more):* [*Assignment: organization-defined system transitional states*]*; upon command by user with appropriate privilege;* [*Assignment: organization-defined frequency*]]; c. Notifies [*Assignment: organization-defined personnel or roles*] of failed security verification tests; and d. [*Selection (one or more): shuts the information system down; restarts the information system;* [*Assignment: organization-defined alternative action(s)*]] when anomalies are discovered.	Substantiated Integrity
136.	SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	The organization employs integrity verification tools to detect unauthorized changes to [*Assignment: organization-defined software, firmware, and information*].	Substantiated Integrity

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
137.	SI-7 (1)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS*	The information system performs an integrity check of [*Assignment: organization-defined software, firmware, and information*] [*Selection (one or more):* at startup; at [*Assignment: organization-defined transitional states or security-relevant events*]; [*Assignment: organization-defined frequency*]].	Substantiated Integrity
138.	SI-7 (6)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION*	The information system implements cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.	Substantiated Integrity
139.	SI-7 (7)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE*	The organization incorporates the detection of unauthorized [*Assignment: organization-defined security-relevant changes to the information system*] into the organizational incident response capability.	Substantiated Integrity, Analytic Monitoring, and Adaptive Response
140.	SI-7 (9)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | VERIFY BOOT PROCESS*	The information system verifies the integrity of the boot process of [*Assignment: organization-defined devices*].	Substantiated Integrity
141.	SI-7 (10)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | PROTECTION OF BOOT FIRMWARE*	The information system implements [*Assignment: organization-defined security safeguards*] to protect the integrity of boot firmware in [*Assignment: organization-defined devices*].	Substantiated Integrity and Coordinated Defense
142.	SI-7 (11)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES*	The organization requires that [*Assignment: organization-defined user-installed software*] execute in a confined physical or virtual machine environment with limited privileges.	Privilege Restriction
143.	SI-7 (12)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY VERIFICATION*	The organization requires that the integrity of [*Assignment: organization-defined user-installed software*] be verified prior to execution.	Substantiated Integrity
144.	SI-10	INFORMATION INPUT VALIDATION	The information system checks the validity of [*Assignment: organization-defined information inputs*].	Substantiated Integrity

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
145.	SI-14	NON-PERSISTENCE	The organization implements non-persistent [*Assignment: organization-defined information system components and services*] that are initiated in a known state and terminated [*Selection (one or more): upon end of session of use; periodically at* [*Assignment: organization-defined frequency*]].	Non-Persistence
146.	PM-12	INSIDER THREAT PROGRAM	The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.	Analytic Monitoring
147.	PM-16	THREAT AWARENESS PROGRAM	The organization implements a threat awareness program that includes a cross-organization information-sharing capability.	Analytic Monitoring Adaptive Response Dynamic Representation
148.	DI-2	DATA INTEGRITY AND DATA INTEGRITY BOARD	The organization: a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and b. Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements123 and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.	Substantiated Integrity

#	Control #	NAME OF CONTROL / CE	Control/Enhancement Text	Relevant Resiliency Technique(s)
149.	DM-1	MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION	The organization: a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection; b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [*Assignment: organization-defined frequency, at least annually*] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.	Non-Persistence
150.	DM-1 (1)	*MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION | LOCATE / REMOVE / REDACT / ANONYMIZE PII*	The organization, where feasible and within the limits of technology, locates and removes/redacts specified PII and/or uses anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.	Non-Persistence Deception

Appendix B References

[1] The MITRE Corporation, "Cybersecurity: Threat-Based Defense," 2013. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/cyber_defense_playbook.pdf.

[2] The MITRE Corporation, "Threat-Based Defense: A New Cyber Defense Playbook," July 2012. [Online]. Available: http://www.mitre.org/work/cybersecurity/pdf/cyber_defense_playbook.pdf.

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

[4] NIST, "Guide for Applying the Risk Management Framework to Federal Information Systems, NIST SP 800-37 Rev. 1," February 2010. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

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

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

[7] The MITRE Corporation, "2nd Annual Secure and Resilient Cyber Architectures Workshop," 1 June 2012. [Online]. Available: https://registerdev1.mitre.org/sr/2012/2012_resiliency_workshop_report.pdf.

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

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

[10] 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," 17 March 2010. [Online]. Available: http://www.ittc.ku.edu/resilinets/papers/Sterbenz-Hutchison-Cetinkaya-Jabbar-Rohrer-Scholler-Smith-2010.pdf.

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

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

[13] M. Cloppert, "Security Intelligence: Attacking the Kill Chain," 14 October 2009. [Online]. Available: http://computer-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain/.

[14] E. M. Hutchins, M. J. Cloppert and R. M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proceedings of the 6th International Conference on Information-Warfare & Security (ICIW

2011), March 2011. [Online]. Available: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf.