MTR170477

MITRE TECHNICAL REPORT

Supply Chain Attacks and Resiliency Mitigations

Guidance for System Security Engineers

Sponsor: NSA/CSS I4
Dept. No.: P522
Contract No.: W56KGU-16-C-0010
Project No.: 0717N871-SC

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

Approved for Public Release; Distribution Unlimited. Case Number: 18-0854.

Bedford, MA

Authors:

William J. Heinbockel
Ellen R. Laderman
Gloria J. Serrao

October 2017

Approved By

/Rosale McQuaid/

Rosalie McQuaid, T8A2, Cyber Resiliency Department Head

19 October 2017

Abstract

Cyber Resiliency Engineering can be applied to systems, missions, business functions, organizations or a cross-organizational mission. In this paper, cyber resiliency is applied to the problem of mitigating supply chain attacks. The adversary's goals for attacking a supply chain are described using the cyber-attack lifecycle framework and the Department of Defense (DoD) Acquisition lifecycle. Resiliency techniques are recommended considering adversary goals and best options to defend against the attacks. The analysis in this document found that the most effective point to apply cyber resiliency mitigations is the *Production and Deployment* phase because this reduces the number of attacks overall. The best place to gain information about adversary targets and activities are both the *Engineering and Manufacturing Development* phase and the *Production and Deployment* phase. An example of how to apply these resiliency techniques is provided based on the Commercial Solutions for Classified capability package for a Wireless Local Area Network (WLAN).

Acknowledgments

The authors would like to acknowledge the expert input from Bob Martin and Peter Kertzner.

The authors would also like to acknowledge the valuable review given by Jenine Patterson, Paul Bicknell, Deb Bodeau, Richard Graubart.

Table of Contents

This page intentionally left blank.

List of Figures

List of Tables

1 Introduction

This report provides analysis and guidance to help Systems Security Engineers (SSEs) supporting Department of Defense (DoD) acquisition programs apply cyber resiliency techniques to supply chain attacks throughout the acquisition lifecycle. The focus is on supply chain attacks against a mission system[1] consisting of information and communications technology (ICT); however, the analysis approach is designed to be extensible to a broader range of mission systems (in particular, those integrating ICT and embedded systems). Cyber resiliency enables an operational mission and the systems which support it to better anticipate, withstand, recover, and evolve despite adversary attacks and other adverse effects.

This analysis can be used by SSEs to apply cyber resiliency techniques and analysis methods throughout the acquisition lifecycle. This will enable programs to develop and execute Program Protection Plans (PPPs) that address cyber supply chain risks effectively, despite such programmatic constraints as reliance on legacy components, components of uncertain provenance, or shared services. SSEs will be able to evaluate how well a given program is applying cyber resiliency throughout the acquisition lifecycle to reduce supply chain risks due to cyber attacks.

To apply these recommendations, Programs need to include requirements motivated by cyber resiliency into contractual documents, specifically Statements of Work (SOWs) and Functional Requirements Documents (FRDs). Cyber resiliency related requirements in SOWs will lead contractors (the Prime or Integration Contractor, the Maintenance Contractor if different, and subcontractors as appropriate) to apply selected cyber resiliency techniques in the design, production, test, and maintenance environments, to make the supply chain more cyber resilient.[2] Cyber resiliency related requirments in FRDs make acquired mission systems more resilient against cyber attacks that exploit weaknesses in the supply chain.

Using the Cyber Resiliency Engineering Framework (CREF) [1] [2], this paper recommends cyber resiliency techniques to address supply chain attacks. Cyber resiliency engineering[3] assumes a sophisticated adversary and an adversary who attacks the supply chain is indeed sophisticated and usually a nation state actor.

In conducting this analysis, the MITRE team leveraged prior work that cataloged forty-one supply chain attacks and associated each one with a phase in the acquisition life cycle [3]. It is important to note that the "target" for these 41 supply chain attacks are predominetly ICT components. An "attack" within the DASD-SE paper is the successful insertion, modification or substitution to/of a component within the supply chain (regardless of whether or not it makes it

[1] A *mission system* is one which directly supports one or more well-defined missions or mission functions; the term is used in this report to avoid confusion with the variety of systems used to support an acquisition program. The mission can be to provide infrastructure or supporting services, as illustrated by the example.

[2] The DoD-published catalog of 41 supply chain attacks [3] includes, for each attack, identification of the attack points (Program Office, Prime Contractor, Subcontractor, Integrator Facility, Software Developer, Hardware Developer, Physical Flow, Information Flow). The importance of defending such systems is also highlighted in Directive-type Memorandum (DTM) 17-001 – Cybersecurity in the Defense Acquisition System [8].

[3] Cyber resiliency engineering is an emerging specialty systems engineering discipline. It is closely aligned with security engineering, safety engineering, and system survivability engineering. It differs from other specialty disciplines in its assumption of advanced cyber threats – Tiers V and VI in the hierarchy defined by the Defense Science Board (DSB) Report on Resilient Military Systems and the Advanced Cyber Threat [30]; its focus on mission assurance rather than on ensuring the conventional security objectives of confidentiality, integrity, and availability; and its use of analytic methods which accommodate the high degree of uncertainty associated with advanced cyber threats.

into an operational system.)   For this paper, these “attacks” are referred to as attack “steps” that are taken to complete a full cyber-attack on the end mission or system, using the Cyber Attack life-cycle.

Grouping these attack steps by their effects on the to-be-acquired mission system (modification, substitution or insertion), we analyzed the number of attack steps that occurred in each phase of the acquisition life cycle. We thus determined the proportion of attack types that occur within acquisition life cycle phases as well as in CAL stages. For example, substitution attack steps are highest in number and happen most often in production and deployment and occur predominately in the pre-exploit phase of deliver. The complete results of this analysis are in Appendix B, and it formed our initial understanding of the adversary’s objectives.

To demonstrate cyber resiliency mitigations against an active cyber adversary, we leveraged existing supply chain risk management (SCRM) guidance but added the perspective of adversary goals and defender goals to describe success (i.e., the adversary’s goals are not achieved and the defenders’ goals are met.) This continuum of actions, reactions, constraint, and adaption to and recovery from adverse attacks (in this case supply chain attacks) is characteristic of cyber resiliency. Through our analysis, we recognized that while the adversary’s ultimate goal is to impact the operational mission system, the adversary will exercise the complete CAL in earlier acquisition lifecycle phases in order to achieve intermediate goals. These intermediate goals include gathering information about mission system development and developing and inserting exploit tools to place hooks in contractor environments for later use.

In Section 2, we introduce key definitions and the frameworks used in our analysis. Section 3 describes the adversary’s goals in attacking a supply chain to exploit a targeted operational environment and describes and provides examples for attacking the systems and components in each stage of the acquisition life cycle.

Section 4 walks through an example using the Commercial Solutions for Classified capability package for a Wireless LAN. It describes the adversary’s goals and possible actions they might take to achieve those goals in this example targeted system.

Section 5 provides our analysis of adversary goals and what a defender hopes to achieve against an adversary’s actions. This analysis leads us to conclude that the most effective point at which to apply cyber resiliency mitigations is the *Production and Deployment* phase because this reduces the number of attacks overall. The best place to gain information about adversary targets and activities are both the *Engineering and Manufacturing Development* phase and the *Production and Deployment* phase. This is where the adversary activity is focused. This section contains recommendations for cyber resiliency mitigations that can be applied to systems throughout the acquisition life cycle and where we believe those mitigations are most effective.

In addition to the recommended mitigations in Section 5, all potentially applicable cyber resiliency techniques are listed in Appendix E, associated with each acquisition life cycle phase, adversary goals and defender goals. These tables serve as a starting point as an SSE analyzes a system for supply chain attacks and the application of cyber resiliency mitigations. SSEs should further tailor this guidance to the specific system or components being assessed and provide security guidance to developers, security architects, security assessments and network defenders. To assist with this tailoring, refer to the example of supply chain attacks on an operational network component (using the Wireless LAN Commercial Solutions for Classified (CSfC) capability package) provided in Section 5.4. This example describes each stage of the acquisition life cycle and applies the most effective resiliency techniques to thwart an attack on the components of this solution.

Finally, Section 6 contains a summary and next steps.

This page intentionally left blank.

2 Background

This section introduces key definitions and frameworks used throughout the paper to characterize supply chain attacks, when they occur, what the adversary wants to accomplish and the best way to defend against them. It also describes the DoDI 5000.02 [4] acquisition lifecycle and the cyber attack lifecycle (CAL). For supply chain, the CAL is used as a structure of a cyber campaign against a mission system where the cyber campaign spans the acquisition life cycle. A large body of work exists on Supply Chain Risk Management (SCRM) and was consulted for this analysis. A subset of this body of work was analyzed and is listed together with their applicability in Appendix C.

2.1 Supply Chain

The Information and Communications Technology (ICT) supply chain is defined in NIST 800-161 [5] as a "linked set of resources and processes between acquirers, integrators, and suppliers that begins with the design of ICT products and services and extends through development, sourcing, manufacturing, handling, and delivery of ICT products and services to the acquirer." This supply chain "can include vendors, manufacturing facilities, logistics providers, distribution centers, distributors, wholesalers, and other organizations involved in the manufacturing, processing, design and development, handling and delivery of the products, or service providers involved in the operation, management, and delivery of the services."

The Defense Science Board (DSB) identifies three interconnected supply chains for DoD weapons systems acquisitions [6]: (1) the global commercial supply chain, which is the source of most microelectronics; (2) the DoD acquisition supply chain, which is designed by the prime contractor; and (3) the DoD sustainment supply chain, which includes aftermarket suppliers. These supply chains are also relevant to ICT systems. For example, the global commercial supply chain also includes sources of commercial off-the-shelf (COTS) software and components (e.g., operating systems, servers, routers). The DoD acquisition supply chain includes systems used by the Program Office to define and track compliance with requirements, systems operated by the Prime or Integration contractor to manage information related to the mission system, systems operated by the Prime or Integration contractor to develop the mission system, and maintenance systems.

2.2 Supply Chain Attack

A **Supply Chain Attack** is defined for this paper as "an intentional malicious action (e.g., insertion, substitution or modification) taken to create and ultimately exploit a vulnerability in Information and Communication Technology (hardware, software, firmware) at any point within the supply chain with the primary goal of disrupting or surveilling a mission using cyber resources." This definition is based on the definition found in [3].

As part of an attack, an adversary wants to achieve success in:

1. inserting malware, tainted hardware, or false information into the supply chain,
2. substituting a bad or corrupt component for a good one, or
3. modifying an existing component to affect its performance adversely (e.g., degrade, deny, make unreliable, or cause to malfunction harmfully).

The Defense Science Board Task Force on Cyber Supply Chain [6] identifies several reasons for the rising importance of supply chain attacks ranging from the increasing complexity of the programmable electronic components to the extended lifetime of system configurations. This report cites the heavy reliance on integrated circuits produced outside the United States and the fact that most PPPs do not carry over to the sustainment phase.

In the DoDI 5200.44 [8] definition of supply chain risk, it states the adversary may "sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system."

This can happen at any phase of the acquisition lifecycle pictured in Figure 1 below. The method of an attacker in this context is to gain access to the supply chain, execute a malicious insertion, substitution, or modification of ICT, and achieve persistence until the altered component is a part of an operational mission and/or system.

This paper focuses on supply chain attacks that are operationally successful. Often a supply chain attack is thought of as successful if the insertion, substitution or modification is completed. However, for true success in the operational environment, an adversary uses the supply chain entry point to control, execute and maintain the software, hardware or firmware containing that malicious modification in order to impact the mission operations.

2.3 DoD Acquisition Lifecycle

The DoD Acquisition Lifecycle ([4], Figure 1) represents a series of phases, separated by milestones and decision points, that an acquisition program moves through from conception to ultimate operational use and disposal. Adversaries can initiate and conduct malicious activities during any and all of these phases. Some of those activities can take the form of supply chain attacks. Ensuring the integrity and security of the supply chain is paramount to the development and operation of a secure and resilient platform. If an adversary can attack the supply chain and taint[4] components, insert malicious compenents into the mission system, or otherwise undermine the ability of the as-delived mission system to meet its requirements, the adversary can compromise the operational system before or during its use.

[4] A "tainted product" as defined in "Open Trusted Technology Provider Standard (O-TTPS) Version 1.1, "Mitigating Maliciously Tainted and Counterfeit Products" is "a product that is produced by the provider and is acquired through a providers authorized channel but has been tampered with maliciously." [28]

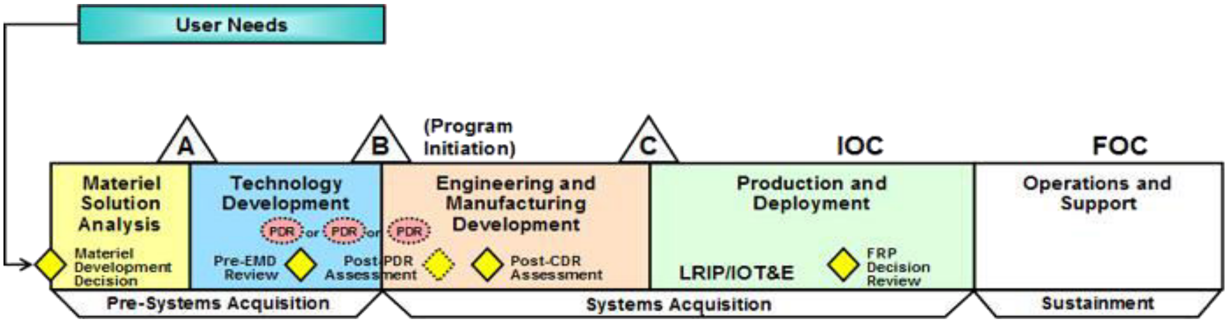

Figure 1. DoD Acquisition Lifecycle

2.4 Cyber Attack Lifecycle

The cyber-attack lifecycle (CAL), first articulated by Lockheed Martin [9] as the "cyber kill chain," depicts the stages of a cyber campaign against a mission system. These stages are what an adversary does to "achieve the objectives of establishing, using and maintaining (or removing) a presence in an enterprise information infrastructure [10]." The stages are shown in Figure 2 below and are:

- Reconnaissance — the adversary gathers information and identifies a target;
- Weaponize — the attack is put in a form to be executed on the victim's system/network (a "cyber weapon" – typically a piece of malware, but in the context of supply chain attacks could also be a tainted software component such as a Dynamic-Link Library (DLL) file or a subverted operating system (OS), a tainted data file, a hardware component which includes malicious logic);
- Deliver — the cyber weapon is delivered to the target system;
- Exploit — the cyber weapon takes advantage of a vulnerability in the target system to install malware;
- Control — the initial installed malware establishes a command and control (C2) channel to the adversary if necessary, and malware propagates from the initial target system more broadly;
- Execute —the adversary achieves the desired cyber effect (which can in turn result in a mission impact); and
- Maintain — long-term access is preserved.

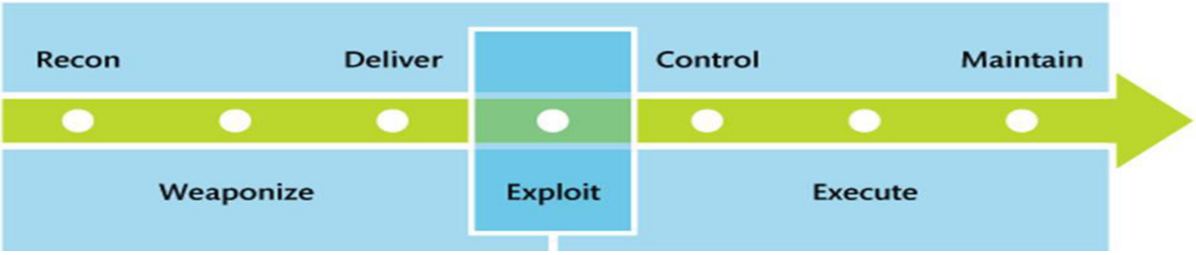

Figure 2. Cyber Attack Lifecycle

Figure 2 shows a single, linear version of the CAL with one end goal and one successful exploit. However, these attack stages are completed multiple times across the acquisition lifecycle, targeted at different systems. Within each phase of the acquisition lifecycle, there are systems and information that can be leveraged by the adversary to attack systems and information in following phases of that lifecycle. For example, the adversary may attack a Program Office system, resource or information in the *Materiel Solutions Analysis* and *Technology Maturity and Risk Reduction phase* to perform reconnaissance and/or start to weaponize (create an exploit for later use.) Then, using that information or "weapon" created, the adversary could execute another attack on the integration contractor's systems in a later phase of the acquisition lifecycle such as the *Production and Deployment* phase. In this case the adversary has cycled through at least two complete CALs as part of the larger CAL directed at the operational mission.

Other forms of a CAL have been defined. In particular, the Office of the Director of National Intelligence (ODNI) has published its Cyber Threat Framework (CTF) [11]. The CTF defines four broad stages of adversary actions: Preparation, Engagement, Presence, and Effect / Consequence[5]; these were used in the DSB Report on Cyber Supply Chain. However, the CTF does not provide enough granularity with respect to the immediate consequences of adversary actions to enable us to analyze which cyber resiliency techniques could be effective against those actions. In addition, the structure of a cyber campaign illustrated above is consistent with NIST SP 800-30R1 [12] and the DoD Guidelines for Cybersecurity Developmental Test and Evaluation (DT&E) [12]. We therefore use the seven-stage CAL illustrated above in Section 3, which provides a good representation of a cyber campaign used across the acquisition lifecycle.

[5] Actions in each stage have defined objectives. Each action has one or more Indicators. Objectives and representative examples of actions are included in the published lexicon. However, these published examples are focused on a mission system in the O&S stage and do not include supply chain attacks.

3 Adversary Goals in the Context of the Cyber Attack and Acquisition Life Cycle

This section details the adversary goals and how an adversary might leverage the CAL at different phases of the acquisition life cycle to impact the operational system and overall mission. It also identifies that the goal of achieving persistence of the "weapon" on the operational environment without detection is a strong motivator for the adversary to use the supply chain as entry onto an operational network. The CAL is recursive and therefore each stage of the acquisition life cycle can be targeted by an adversary and the entire CAL can be executed within any or all of acquisition lifecycle phases. This document is focused on showing the bigger picture of how the CAL is used over the entire acquisition lifecycle, the impact on the *Operations and Support* phase of the acquisition lifecycle, and the cyber resiliency mitigations that can be applied to reduce or eliminate these impacts. This focus does not imply that addressing the full CAL within each acquisition lifecycle phase is unnecessary or not as useful; it is just not the focus of this paper.

3.1 Primary Goals

An adversary using supply chain attacks against a mission system can have any of a variety of goals, related to the mission, to the information handled by the system, or to the role of the system or mission in a larger context [14]. In the abstract, the primary goal of the adversary is to impact confidentiality, integrity, and/or availability (CIA) of an end system and, ultimately, the mission it supports. To accomplish this, the adversary carries out the stages of the CAL (e.g., exploit, control, execute, and maintain), as referenced in Section 2.4, above. This means our analysis approach may be applied to a wide range of missions. Possible cyber effects[6] on the mission system include:

- Violate Confidentiality (intercept): gain unauthorized access to information;
- Reduce Integrity (modify, fabricate): cause the system to malfunction; cause end users to mistrust the information and information system; or cause end users to do unintended things (e.g., friendly fire);
- Reduce Availability (degrade, interrupt): making the system and information or resource unavailable when it is needed; or,
- Use resources for illegitimate purposes (unauthorized use or usurpation): use for potentially harmful reasons and violate the confidentiality, integrity, or availability of other resources that trust the information asset being attacked by the adversary (as they don't know it is compromised).

In line with the focus of this analysis on *Operations and Support*, this section describes what an adversary wants to achieve in each stage of the acquisition life cycle in order to exploit the final mission system.

It is recognized that adversaries will also attack systems within each life cycle stage. Systems and environments, for example those that produce system design requirements or support acquisition and development of a final mission system, are subject to attack. Many of the cyber

[6] The words in parenthesis come from [10].

resiliency techniques recommended here can also be applied to systems whose mission is to develop, purchase or maintain another operational mission system.

3.2 Achieving Goals by Actions Taken throughout the Acquisition Life Cycle

As identified by our analysis of supply chain attacks, attacks are most effective when started in earlier stages of the acquisition life cycle [3] and continue through all stages to *Operations and Support*. For example:

- During the *Materiel Solution Analysis* Phase and the *Technology Maturity and Risk Reduction Phase*, the adversary is focusing on Reconnaissance — that is, finding out as much as possible about the mission needs, functional requirements, and expected technical architecture of the mission system for later use. The adversary is mainly targeting the Program Office during this phase.
- In the *Engineering & Manufacturing Development* phase and the *Production & Deployment* phase, the adversary is doing more reconnaissance, developing weaponized tools, delivering them to the environment and executing the initial exploit (getting their hooks into applications and systems). The adversary is mainly targeting contractor systems (both prime and subcontractor) during this phase
- If the adversary attack is successful, during the *Production & Deployment* phase and the *Operations & Support* phase the adversary achieves their goal of controlling weaponized tools, executing the attack and maintaining their presence for further attacks. During this phase the adversary is targeting contractor systems, integrator facilities, software and hardware development, as well as the physical flows and information flows.

Figure 3 below is a representation of the ways an adversary moving through the stages of the CAL might interact with the acquisition lifecycle. An individual adversary attack may not necessarily target each acquisition phase using every stage in the CAL shown in ; however, since each acquisition phase could be targeted as part of an extended campaign against the final mission system, resilience against those attacks and adverse effects should be considered within that acquisition phase. This mapping reflects stages in the acquisition lifecycle where the adversary will focus their efforts to achieve their desired CAL objectives, rather than a description of a specific attack flow. The adversary may choose to go beyond these focus areas. A different perspective of the acquisitions-CAL relationship is shown in Table 2 below.

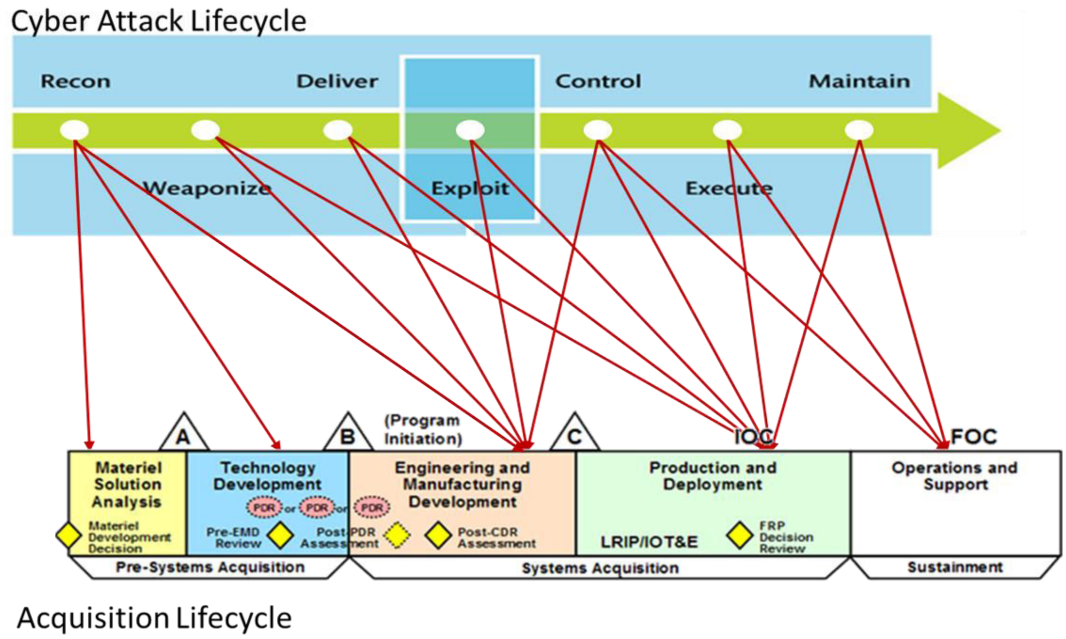

Figure 3. Cyber Attack Lifecycle in the Context of the Acquisition Lifecycle

For the remainder of this paper, the adversary goals with respect to the mission system will be referenced as shown in the Table 1. below. This allows for a clearer understanding and application of the CAL to the action an adversary wants to achieve in that stage of a supply chain attack.

Table 1. Cyber Attack Lifecycle and the Associated Adversary Goals

Recon	Weaponize	Deliver	Exploit	Control	Execute	Maintain
Acquire information	Develop tools for attack (craft a “cyber weapon”)	Deliver the cyber weapon	Take advantage of a vulnerability to install the cyber weapon, making it part of the mission system	Control the attack in the mission system environment	Achieve the intended effects on the mission system	Maintain presence for future attacks

The Table 2 below shows the actions the adversary wants to accomplish (goals) for each phase of the acquisition life cycle and each stage of the CAL with example target systems listed. To accomplish these goals, the adversary would execute the full CAL against the target system(s).

Table 2. Adversary Goals, the Acquisition Lifecycle and the Cyber Attack Lifecycle

Acquisition Lifecycle Phase	Associated Cyber Attack Lifecycle Stage	Target System Examples	Adversary Goals with Respect to Mission System
Materiel Solutions Analysis	Reconnaissance	Program Office systems handling information about needs, concept of operations, interfaces	Acquire information about the to-be-acquired mission system

Acquisition Lifecycle Phase	Associated Cyber Attack Lifecycle Stage	Target System Examples	Adversary Goals with Respect to Mission System
Technology Maturity and Risk Reduction Phase	Reconnaissance	Program Office systems handling information about technical alternatives, risks	Acquire information from design review
Engineering & Manufacturing Development	Reconnaissance	Program Office, contractors and subcontractor systems handling information about design decisions and implementation processes	Acquire information about technical architecture of mission system
	Weaponize	There are no target system examples because this activity takes place on an adversary system using information gained in previous stages	Develop cyber weapon, based on expected technical architecture of the mission system
	Deliver	Contractor and sub-contracter systems used to manage and execute design and implementation processes	Deliver the cyber weapon – get the cyber weapon / malicious component into the contractor's development environment, so that it will be integrated into the mission system
	Exploit	Contractor and subcontractor systems used to manage and execute design and implementation processes	Take advantage of a vulnerability to install the cyber weapon, i.e., to make it part of the mission system
	Control / Maintain	Contractor and subcontractor systems used to manage and execute design and implementation processes; Program Office systems handling information from design reviews	Prevent the detection of the insertion of the cyber weapon into the mission system – undermine contractor quality assurance processes and tools to prevent the insertion of the malicious component from being detected.
Production & Deployment	Weaponize	*There are no target system examples because this activity takes place on an adversary system using information gained in previous stages*	Develop cyber weapons based on technical architecture and identified characteristics of the mission system (e.g., specific products or components)
	Deliver	Contractor and subcontrator systems used to manage and	Deliver cyber weapons – get the cyber weapon / malicious

Acquisition Lifecycle Phase	Associated Cyber Attack Lifecycle Stage	Target System Examples	Adversary Goals with Respect to Mission System
		execute design and implementation processes; COTS supply chain for previously identified components	component into the contractor's development environment, so that it will be integrated into the mission system
	Exploit	Contractor and subcontractor systems used to manage and execute design and implementation processes; COTS supply chain for previously identified components	Take advantage of a vulnerability to install the cyber weapon, i.e., to make it part of the mission system
	Control / Maintain	Contractor and subcontractor systems used to manage and execute design and implementation processes	Prevent the detection of the insertion of the cyber weapon into the mission system – undermine contractor quality assurance processes and tools to prevent the insertion of the malicious component from being detected
	Execute	Execute malware so it successfully corrupts or otherwise undermines critical contractor developed systems	Execute malware the defender's environment in the deployed system before being migrated to *Operations and Support*
	Maintain	Systems used in test and evaluation, at prime contractor, independent validation and verification (IV&V) organization, or cyber range	Prevent the detection of the insertion of the cyber weapon into the mission system – undermine quality assurance processes and tools to prevent the insertion of the malicious component from being detected; modify test results
Operations & Support	Control	Mission system	Control the Attack in the Mission System Environment
	Execute	Mission system	Achieve the intended effects on the mission system
	Maintain	Mission system; systems used for maintenance and support	Maintain Presence for Future Attacks

3.3 Example Adversary Actions

This subsection discusses example actions of attacks at each acquisition phase in the abstract. Section 4 provides a notional example that is more specific. These attacks, typically employ common cyber attacks along with coordination across multiple attacks, are part of the larger, recursive, cyber attack lifecycle described in Section 3.2.

In the *Materiel Solutions Analysis* and *Technology Maturity and Risk Reduction Phases*, the adversary is focused on reconnaissance – trying to find out about the end system. The reconnaissance activities the adversary most likely uses in these phases are extremely hard to detect because they are frequently passive (e.g., collecting data by listening to traffic on a network) or hidden (e.g., hiding information exfiltration in normal network traffic). These activities can still be mitigated against by using one or more of the techniques described in section5. Addressing the reconnaissance activities in the *Materiel Solutions Analysis* phase and the *Technology Maturity and Risk Reduction phase* is one of the most effective ways of addressing the adversary's weaponization activities. If the adversary does not have adequate information it is hard for them to develop effective weaponized tools.

The adversary focuses their weaponization, attack delivery, and installing the exploit in the *Engineering and Manufacturing Development* Phase and the *Production and Deployment* phase. There is also further reconnaissance to determine what to do in this and later acquisition lifecycle phases. Examples of these types of attacks include[7] microprocessors or other chips with secret back doors substituted for legitimate hardware components, malicious code inserted into open source software libraries, and establishing rogue processes in an integration facility to clandestinely insert maliciously altered components.

The adversary shifts towards Control, Execute and Maintain activities as the acquisition lifecycle progresses into the *Production and Deployment* phase and the *Operations and Support* phase. By the *Production and Deployment* phase, the adversary already has a foothold in the mission system. While the adversary is likely still developing or honing their weapons, delivering new versions or updates, and initiating new attacks; their interests have transitioned to controlling their tools, executing the attack on the mission, and maintaining their presence (e.g., when the system goes through independent verification and validation). This is particularly true as the system moves towards the later portion of the phase. Some examples of what the adversary might do are: corrupt critical operational data by injecting false but believable data into the system during configuration[8], or leverage backdoors previously inserted into software or compromised hardware or firmware to control systems.

During the *Operations and Support* phase, the adversary focuses on Control, Execute and Maintain activities. The adversary may trigger their backdoors to establish C2 channels. Alternately, their cyber weapon could be set to auto-trigger based on conditions that can be detected within the mission system.

3.4 Adversary Advantages Gained Via Supply Chain Attacks

As stated above, when employing a supply chain attack, the adversary wants to impact confidentiality, integrity, and/or availability (CIA) of critical mission systems so as to affect the mission which depends on those systems. Supply chain attacks, just like any cyber attack,

[7] Attacks A6, A 27 and A29 from [3] are examples of this type.

[8] Attack A37 from [3]is an example of this type of attack.

exploit a target system and then seek to control, execute and maintain presence on that system. So, a supply chain attack once delivered, will appear to a network defender like any other cyber-attack. It will use the same tactics, techniques and procedures (TTPs) (establish persistence, gain credential access, lateral movement etc.). In their delivery, however, supply chain attacks are unique and the adversary has the advantages of establishing persistence early by embedding the attack within one component of the end mission system and delivering the cyber weapon undetected. Cyber-attacks are, for the most part, delivered from an external source to an operational network. Therefore, perimeter defenses such as intrusion detection devices and firewalls are effective tools to detect and stop attacks upon entry. However, a supply chain attack is often initiated by an embedded change to a component of the system which is accepted as a "known good." An approved or "trusted" delivery mechanism such as a software update function delivers the supply chain attack unsuspected by a network defender. As stated in the recent Defense Science Board Task Force on Cyber Supply Chain "when done effectively, malicious insertion will not be detectable until actuated and it may present as a design flaw when ultimately observed [6]."

The supply chain attack is initiated early in the system design so that persistence can be established before the system is built. Once present in a low-level component such as firmware, a supply chain attack is difficult to detect on an operational network and is a key advantage of supply chain attacks.

A recent example of an attack in which the software supply chain was compromised is Nyetya (Cisco TALOS naming convention) or NotPetya (widely known name) ransomware of late June 2017. This ransomware, per preliminary reports, did not gain access via an email or office document. Instead, the entry point is thought to be via the update system for a Ukrainian tax accounting package (MeDoc) [15]. Once entry was gained, the adversary enumerated the network components, stole credentials, moved laterally eventually encrypting large amounts of information.

Another example of an effective supply chain attack is a Basic Input Output System (BIOS) implant. This implant can be done at a point within the supply chain prior to operations or by an automated firmware management function such as Intel Active Management Technology or Intel Standard Manageability (AMT, LMS) that operate below the OS (unobservable from OS/kernel). A BIOS or unified extensible firmware interface (UEFI) implant establishes presence and maintains that presence even if the operating system is re-installed.

In summary, supply chain attacks can be distinctive in their delivery methods. They provide an advantage for achieving undetectable delivery and early persistence.

This page intentionally left blank.

4 Notional Example of Supply Chain Attack

This section describes an example of a supply chain attack in the context of the acquisition lifecycle, detailing the steps throughout each acquisition phase and the ultimate impact in the *Operations and Support* Phase. In this notional example, a wireless local area network is to be acquired and deployed at a campus (e.g., a military base or a set of buildings in a metropolitan area).

We examine a supply chain attack within the context of the Campus Wireless Local Area Network (WLAN) Commercial Solutions for Classified (CSfC) Capability Package (CP) [16]. The intent of this CP is to minimize the risk of wireless devices accessing sensitive data and enterprise service domains. Figure 4 shows an example deployment of the capability that supports wireless access to multiple classification domains.

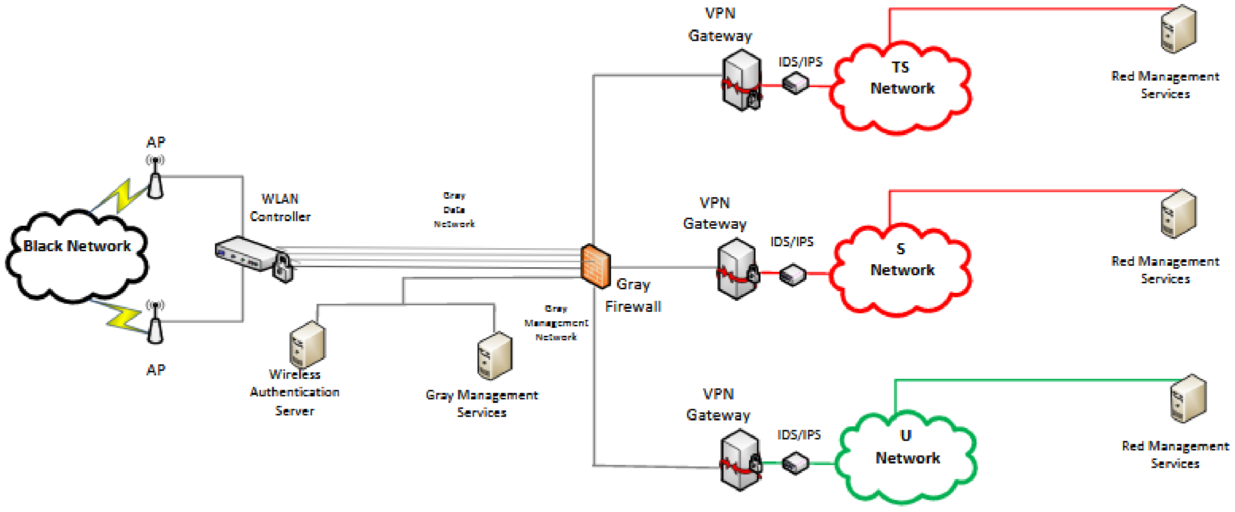

Figure 4. Multi-level Domain Campus WLAN Solution

During the early stages of the acquisition – i.e., the *Materiel Solutions Analysis* and *Technology Maturation and Risk Reduction* phases, the acquiring organization identifies capabilities and mission system-level requirements, including the requirement for wireless access to multiple classification domains. The acquisition team identifies several plans for such architectures, including the Campus WLAN CP. An adversary would want to engage in this phase primarily for reconnaissance. Initial capabilities and requirements documents (e.g., ICD, CDD) hold valuable information such as key performance parameters (KPPs) and key system attributes (KSAs), that can give adversaries insight into potential designs or likely product choices. For example, the number of simultaneous users or VPN performance requirements may limit the number of product options. With this information, adversaries can begin to target those specific technology vendors and start researching potential vulnerabilities.

In addition to reconnoitering, adversaries may also have opportunities to influence requirements to degrade the overall security or survivability of the mission system. Adversaries may engage by directly accessing and modifying the files or by targeting acquisitions personnel to convince them to make the necessary changes. This might be done by planting information that certain vendors are experiencing product difficulties.

During the *Engineering & Manufacturing Development* phase, the technical planning and development gets underway. External personnel are brought in through contracts for capability development and integration. For the WLAN CP requirements, the acquiring organization starts to specify the architecture and develop the initial hardware and software designs. The Acquisitions Office also begins to identify the appropriate cybersecurity and resiliency needs (Figure 5).

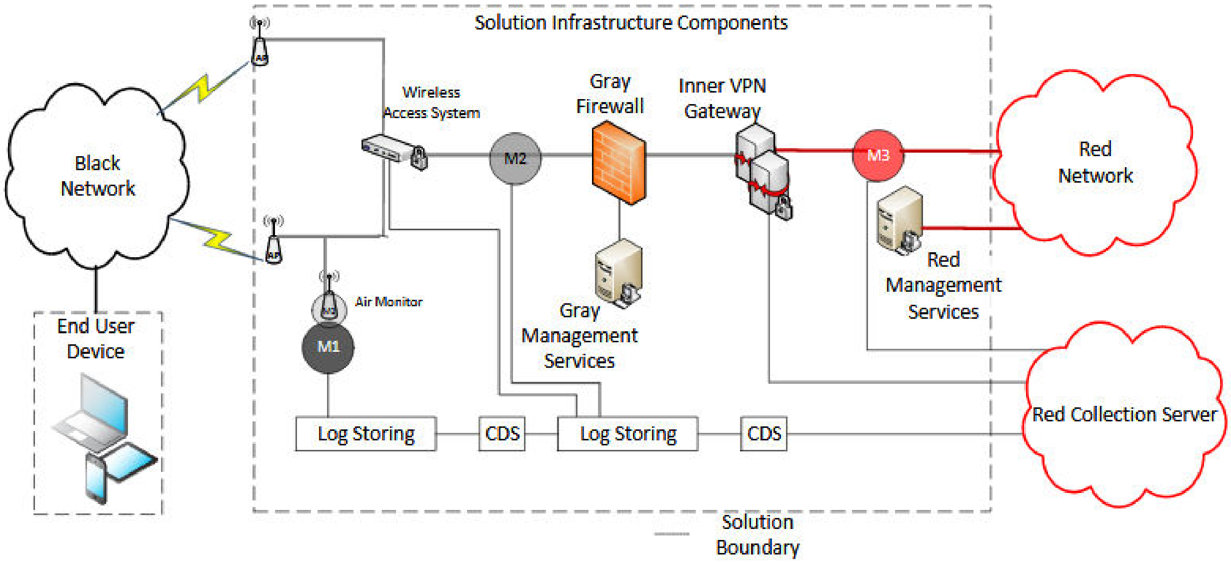

Figure 5. Example Campus WLAN Continuous Monitoring Points

These activities translate to increased opportunities for an adversary. As the acquisitions shift from soft requirements to hard deliverables, the adversary can begin weaponizing and delivering exploits for eventual integration. Adversaries may target the design specifications for specific hardware and software components. They will look for weaknesses in the system's defense and survivability capabilities such as flaws in the VPN or wireless frequencies that can be exploited. They may reverse engineer potential safeguards and verification capabilities. Defensive cyber operations pose an interesting supply chain target for adversaries, as the defenses are usually monitored less and are not considered mission essential, but are often deployed in line with more critical components.

Additional external involvement of people and organizations only increases the attack landscape. Instead of targeting the more protected and aware program office, the adversary can focus on the primary and secondary contractors. The farther the supply chain level is from the acquisition organization (e.g., subcontractors, component suppliers), the more likely an adversary will be able to successfully target as their OPSEC requirements are likely to be less stringent. Instead of going after the prime WLAN CP integrator, the adversary may engage or otherwise target the subcontractor providing the WLAN access points or the supplier of the authentication management software (e.g., as a front company).

As acquisitions shifts into the *Production & Deployment* and *Operations & Sustainment* phases, the adversarial tactics transition to the more typical supply chain attacks against the components. While the acquisition activities in *Production & Deployment* and *Operations & Sustainment* are different, adversaries will target the supply chain in similar ways to implant and modify components. *Production & Deployment* is an inject point for counterfeit hardware components, but similar opportunities present themselves in *Operations & Sustainment* through testing, troubleshooting, and periodic upgrade or refresh cycles. A determined adversary will examine the supply chain to attack the weakest points, regardless of whether it is hardware, firmware, or software.

Another potential supply chain attack vector is through the configuration. Even a small environment such as the WLAN CP has multiple configurations to enable authentication and access management. These include WLAN access lists, VPN configuration and authentication lists, gray management service configurations, firewall rules, IDS/IPS rules, and network appliance and routing rules. Configuration files are rarely modified and less likely to be persistently monitored. Most often, the configurations are brought in from a contractor development lab via a test facility, or through an external vendor. As it would be evident if an adversary were to tamper with the configuration to degrade the environment, they could use configurations to expand the system attack surface by enabling other capabilities or disability security services. Enabling weaker crypto mechanisms on the wireless signals or VPN may be just enough for the adversary to gain access to an otherwise secure WLAN.

This page intentionally left blank.

5 Cyber Resiliency Mitigations for Supply Chain Attacks

The previous sections described adversary intentions and methods and examined them through the wireless LAN example. This section recommends cyber resiliency techniques to mitigate adverary attacks on the supply chain. This section introduces cyber resiliency mitigations, defines a set of goals for a defender, and then recommends resiliency techniques and approaches that can best achieve the defenders' goals to thwart supply chain attacks throughout all stages of the acquisition lifecycle. The recommended mitigations are listed in the below text. In addition, tables in Appendix D contain a more extensive list of cyber resiliency mitigations and what adversary goals are thwarted and what defender goals are achieved for each.

The SSE combines their knowledge of the specific system under review and the deployment environment, with known adversary tactics and techniques. This section can then be used to cross-reference that information with the appropriate cyber resiliency techniques to augment traditional security solutions (e.g., redundancy, privilege restriction, substantiated integrity) and those that add less traditional cyber resiliency techniques (e.g., diversity, deception, dynamic positioning) that can change the attack surface [17]. The authorizing official should also consider cyber resiliency in making a risk management judgment and trying to reduce risk to an acceptable level.

5.1 Cyber Resiliency Summary

Cyber resiliency (also referred to as cyber resilience) can be defined as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources."[9] Appendix D "Summary of Cyber Resiliency Techniques and Approaches" summarizes candidate mitigations for achieving cyber resiliency against supply chain attacks.

It is not feasible to apply all cyber resiliency techniques to an architecture, so the system architect is compelled to select the most effective subset of those techniques while considering the impact on the overall system. Some considerations when selecting cyber resiliency techniques are:

- How the technique addresses the types of risks in the architecture under consideration
- The relative maturity and readiness for cyber resiliency application
- The potential interactions between the techniques – both conflicting and synergistic
- The effects on the adversary[10]
- Additional political, operational, economic and technical (POET) factors.

It is not possible to adequately incorporate these considerations in an assessment without a specific architecture and environment. Cyber resiliency techniques are focused on achieving one or more cyber resiliency objectives.[11] In addition, some techniques work better in certain types of architectures than others. For this reason, the discussion here is focused on applicability and will also discuss the interactions between, the resiliency techniques but will not discuss the specific POET factors.

[9] Cyber resources are "Separately manageable resources in cyberspace, including information in electronic form, as well as information systems, systems-of-systems, network infrastructures, shared services, and devices." - derived from [9].
[10] Appendix A provides a brief discussion of the potential effects on the adversary using the cyber resiliency approaches described in this paper. These are discussed in more detail in Table H-6 of [18] and in [33].
[11] Cyber resiliency objectives are described in [2].

The reader should consult Appendix D: "Summary of Cyber Resiliency Techniques and Approaches" as background information before reading the following sections. It is key to understanding the cyber resiliency techniques and approaches recommended in this section.

Because the following discussion applies to missions in general, Section 5.2 will discuss defender goals in general terms and the resulting recommendations need to be tailored when applying them to a mission. This is so that the resiliency needs of that specific mission are addressed. Section 5.3 provides a more detailed description of specific recommendations based on environmental factors. Section 5.4 will show how resiliency mitigations might be tailored for a specific environment by revisiting the example attack described in Section 4.

The application of cyber resilience mitigations to supply chain attacks must take both the threat environment and the mission environment into account. The discussion in Section 3 described the threat in terms of adversary actions in the abstract, while the discussion in Section 4 described the threat in terms of adversary actions in a theoretical environment.

5.2 Defender Goals

The overall defender goal is to enable missions to succeed despite being under attack. In some situations, the mission is a single event. More frequently the mission is ongoing and the defenses must evolve as the adversary's attack evolves. This defense is supported by four underlying defender activities.[12] Just as with attacker goals, each defender goal is supported by a different combination of cyber resiliency mitigations. The defender goals are:

- Reduce Attacks: While defenders cannot eliminate all attacks the number and range of attacks in the *Operations and Support* phase can be reduced by cyber resiliency mitigations in earlier phases of the acquisition lifecycle.
- Diminish Success of Attacks: Cyber resiliency mitigations applied throughout the acquisition lifecycle can make attacks that are not eliminated less successful. This can mean either limiting the overall impact to the mission or limiting the impact on the specific element of the environment being attacked.
- Gain and Share Information about Adversary Activity: Sharing information about adversary activity throughout the acquisition provides knowledge of adversarial activities within the *Operations and Support* phase. Defenders can use the information acquired from adversary activities in prior acquistion phases to detect and stop attacks as well as to change mission operations so that attacks do not stop the mission.
- Recover: Using information gained from earlier phases along with appropriate preparations, helps defenders achieve recover operational abilities quickly enough to ensure the mission is accomplished.

For this analysis, we provide a general characterization of defender activities undertaken to enable mission success. It should be noted, however, that defenders' focus may differ based on their role within an acquisition lifecycle phase. For example, early in the acquisition lifecycle, the defender is the service element which provides ICT support to the Program Office. The

[12] These acctivities are associated with the effects on threat events described in Appendix H of NIST SP 800-160 [18]. Reducing an attack covers the categories of "Redirect", "Preclude" and "Preempt"; limiting the effectiveness of attacks covers the categories of "Impede" and "Limit"; and gaining and sharing information covers the categories of "Detect" and "Expose".

defender is focused on preventing exfiltration of sensitive information about the system to be acquired, and preventing specifications from being modified.

Later, in the acquisition lifecycle (during the *Engineering and Manufacturing Development* and *Production & Deployment*), the defender is the prime contractor, together with subcontractors and suppliers. The overall goals are to prevent exfiltration and to prevent unauthorized modification – of specifications, design documents, and to-be-deployed-system components.

During the *Operations & Sustainment* phase, two defenders are active: the defender of the as-deployed system, and the defender of the maintenance environment. The defender of the as-deployed system is focused on mission assurance; the defender of the maintenance environment is focused on protecting the portion of the supply chain for which they are responsible.

The "recover" goal is usually part of "limiting" the effectiveness of attacks as refered to in [18]. In the case of supply chain attacks the difficulty of recovery and the need to specifically focus on that aspect makes it appropriate to emphasize this goal along with the other three.

5.2.1 Effective Defense Throughout the Acquisition Lifecycle

Defenders can more effectively address adversary activity if they defend the acquisition lifecycle as a whole, rather than viewing each phase in isolation without sharing information or considering the other phases. This is challenging because the environment and its ownership (e.g., program office, contractor, or mission environment) changes as the acquisition lifecycle progresses. The *Engineering and Manufacturing Development* and *Production and Deployment* phases provide the greatest opportunity for defenders both in terms of Cyber resiliency techniques and approaches (i.e., greatest number of techniques possible) as well as in terms of impact across the goals (i.e., the adversary has the most widely varied activity and is most active in these phases). In addition, if defenders wait until *Operations and Support* to address the adversary's threat to *Operations and Support*, the adversary has already acted and the possibilities of remedy are limited because the environment is less flexible.

As the system moves through the acquisition lifecycle, the adversary priorities change from obtaining information about the system to developing and delivering initial exploits to get hooks into the development environment and the finally to attacking the end system and maintaining control. Similarly, as the system moves through the acquisition lifecycle, the defender priorities should shift from protecting information to protecting the component development environment and gaining information about the adversary for defense activity in *Engineering and Manufacturing Development* and *Production and Deployment* and finally to detecting and responding to adversary activity in *Production and Deployment* and *Operations & Sustainment*. More specifically, the set of potential cyber resiliency mitigations increases over the acquisition lifecycle to include:

- Protecting information from unauthorized access
- Analyzing what the adversary is doing, detecting their presence,
- Making it harder for the adversary to function in the development environment by making it more diverse and deceptive,
- Responding to the adversary activities in such a way that it minimizes the adversary's ability to
    - successfully complete an attack and
    - cause the adversary to expose their activities as much as possible.

Based on the adversary activities as described in [19], the most effective points at which to apply the cyber resiliency mitigations to reduce the number of attacks in the *Operations and Support* and gain the most information about adversary targets and activities are in the *Engineering and Manufacturing Development phase* and the *Production and Deployment*.

5.3 Cyber Resiliency Mitigations Considering Adversary and Defender Goals

Cyber resiliency countermeasures are any response taken to prevent, mitigate, or recover from one or more attack impact.

- Preventative countermeasures reduce the likelihood of an adverse event or subsequent effect by avoiding or preventing the initial attack vector.
- Mitigating countermeasures constrain or otherwise decrease the rate of degradation caused by the adverse impact.
- Recovery countermeasures improve the rate of reconstitution, such as through restoring lost capabilities or making additional resources available.

Countermeasures can occur across people, processes, technology, and policy. The information gained from these countermeasures can be used to evolve the mission operations and systems, increasing cyber resiliency.

Below is a discussion of cyber resiliency countermeasures that can be used to mitigate the operational impacts caused by successful supply chain attacks. The most widely applicable and effective mitigations will be highlighted in this text. The rest can be found in the tables in Appendix D.

5.3.1 *Materiel Solutions Analysis* Phase

In the *Materiel Solutions Analysis* phase, the adversary goal is to gain information. Defenders are usually not able to gain specific information about adversary interests because of the passive techniques used by, and the adversary's diverse interests at this point in their attack lifecycle. In general, defender environments tend to be enterprise IT and techniques such as *Non-Persistence*, *Privilege Restriction* and *Segmentation* are the best ways of defending against the adversary activities in this phase.

Specifically, the *Non-Persistence Information* approach wipes information as soon as it is no longer needed. This approach can be applied to information caches and other temporary information storage areas. *Non-Persistent Services* and *Non-Persistent Connectivity* approaches remove the services and connectivity respectively when they are not being used for authorized purposes thereby denying paths to the information. All three approaches reduce the opportunities for unauthorized access to information.

The *Privilege Management* approach of the *Privilege Restriction* technique reduces the number of resources accessible with individual resources based on criticality. Within the *Material Solutions Analysis* phase, this causes the adversary to spend more effort to gain access credentials to the resources most useful in gaining reconnaissance information. Similarly, the *Privilege-Based Usage Restriction* approach reduces the opportunity for the adversary to gain access to resources by restricting access to only those individuals who need a resource to perform their duties. With this approach in place, the adversary must spend additional effort in identifying which individuals have access to the resources they need. The *Dynamic Privileges* approach is one that changes the level of privileges assigned to users as well as the level of privileges needed to access resources dynamically. For example, access to certain resources after regular work hours could be restricted to a smaller group of people, thereby making it harder for the adversary to conduct activities at times they would not be noticed.

There are two *Segmentation* approaches – *Predefined Segmentation* and *Dynamic Segmentation* – that are useful within the *Material Solutions Analysis* phase. Both these approaches reduce the adversary's ability to exfiltrate data defeating their main goal in this phase.

In addition, using the *Temporal Unpredictability* approach of the *Unpredictability* technique in conjunction with *Privilege Restriction* can boost that technique's effectiveness by making it even more difficult for the adversary to determine which privileges are needed at a specific time. For more details please refer to Appendix C.

5.3.2 *Technology Maturity and Risk Reduction* Phase

Recommendations for mitigations within the *Technology Maturity and Risk Reduction phase* are like those in the *Materiel Solutions Analysis* phase. However, there is more specificity in this phase. The defenders are more focused on solutions and the adversaries may have made some choices about what technology to investigate further. For these reasons, the *Deception* technique is added to the recommended techniques to consider. There are three approaches – *Obfuscation, Dissimulation/Disinformation* and *Misdirection* – that are included within the *Deception* technique that are applicable to the *Technology Maturity and Risk Reduction phase*. *Obfuscation* (i.e., encryption) makes it difficult for the adversary to identify and target high value information resources. *Dissimulation/disinformation* purposely provides the adversary with false information so that attacks developed for later phases are ineffective. *Misdirection* wastes the adversary resources by directing them to deception environments (*i.e.,* honeynets).

5.3.3 *Engineering and Manufacturing Development* Phase

During the *Engineering and Manufacturing Development* phase the initial exploit may occur. The adversary goals expand to developing and delivering this exploit, initiating it and then controlling the subsequent attack. With a more active adversary, the defenders can gain information about the adversary in addition to reducing and limiting the attacks that reach the *Operations and Support* phase. In addition to the *Deception* technique, the *Analytic Monitoring* technique can be effective in gathering information to share with later phases of the acquisition lifecycle. Both *Substantiated Integrity* and *Non-Persistence* techniques can make it difficult for the adversary to deliver an exploit, hopefully reducing the number of attacks. *Substantiated Integrity* provides mechanisms for checking whether resources such as critical services, information stores, information streams and components have been corrupted. *Non-Persistence* provides opportunities to refresh those critical resources from known good sources. The *Non-Persistence* technique also reduces the time resources are available to be attacked. When these two techniques are combined with the *Unpredictability* technique, the adversary's ability to create accurate and precise plans decreases, thus reducing the number of attacks that later appear in the *Operations and Support* phase of the Acquisition Lifecycle.

Sensor Fusion and Analysis is an approach within *Analytic Monitoring* that helps expose adversary activity. Defenders use monitoring data and preliminary analysis results from various components and integrates this information with external threat intelligence to identify potential or actual adversary activity. The *Malware and Forensic Analysis approach* to *Analytic*

Monitoring focuses on known adversary activities and artifacts to identify the presence and activities of the adversary. Both approaches provide information that can be used to eliminate the initial exploit and follow-on control exerted by the adversary. The information gained using this technique can also be shared with later acquisition lifecycle phases and make it easier for the defender to make effective recovery plans.

The *Non-Persistence* approaches described above can be used in the *Engineering and Manufacturing Development* phase to reduce the adversary's ability to deliver, initiate and control attacks by reducing the paths into the environment through the *Non-Persistent Services* and *Non-Persistent Connectivity* approaches. The *Non-Persistent Information* approach can be implemented by reimaging the environment from known clean images.

The *Substantiate Integrity* technique approaches – *Integrity Quality Checks*, *Provenance Checking,* and *Behavioral Validation* – are all useful in ensuring that the "clean" images referenced in the previous paragraph are indeed clean and reimaging the environment with these images will not cause the adversary to persist.

As previously described, the approaches within the *Unpredictability* technique can be used to increase the effectiveness of other approaches. Within the *Engineering and Manufacturing Development* phase, defenders can combine *Temporal Unpredictability* with the *Non-Persistence* approaches to increase the uncertainty for the adversary. For example, the adversary will have a much more difficult time executing successful attacks and remaining undiscovered if they are uncertain about how long a service will be available, a connection will stay open or their exploit will remain in the environment. Likewise, combining *Contextual Unpredictability* with integrity quality checks makes it more difficult for the adversary to emulate components and get compromised components into fielded systems.

5.3.4 *Production and Deployment* Phase

The *Production and Deployment* Phase is an attractive target for the adversary because this phase has the most mature products prior to the *Operations and Support* phase but the safeguards that are in the *Operations & Support* phase may not be in place in this environment. If the defenders – the prime contractors and subcontractors – are using cyber resiliency techniques such as *Analytic Monitoring, Deception*, and *Dynamic Representation,* there is a high likelihood that they will be able to identify and understand adversary behavior. Even if they are unable to completely stop the adversary activity, they will be able to gather information and share it with the *Operations & Support* phase environments so that they are better able to limit the impact of the attacks there. In addition, it may be easier to stop or limit the attacks in the *Production and Deployment* phase with techniques such as *Adaptive Response* because there may be more flexibility in this phase than in the operational environment. Likewise, some aspects of *Coordinated Defense* and *Diversity* techniques may be easier prior to the operational environment.

The approaches within the *Dynamic Representation* technique – *Dynamic Mapping & Profiling, Dynamic Threat Modeling,* and *Mission Dependency & Status Visualization* are focused on constructing and maintaining representations of the environment or mission in light of cyber events and actions (both adversarial and defense). The *Dynamic Mapping & Profiling* approach identifies software and components that do not conform to policy requirements or that are behaving in unexpected ways. The *Dynamic Threat Modeling* approach reveals patterns and trends in adversary behavior and the *Mission Dependency & Status Visualization* approach identifies consequences of adversary execution. The information gained from these approaches can be combined with the other information used in *Analytic Monitoring* along with information gained from *Deception* activities to increase the likelihood of identifying and understanding adversary behavior and targeting for this Acquisition Lifecycle phase as well as *Operations and Support*. With this information, recovery plans for the *Operations and Support* phase can be defined and tested.

5.3.5 *Operations and Support* Phase

Once the Acquisition Lifecycle has moved into the *Operations and Support* phase, there is frequently less flexibility in what mitigations can be employed as well as limits on what the mitigations can do. The malware will already have been implemented in the targeted mission system so it is harder to preclude an attack in this phase. For example, because the environment may not be flexible, the ability to deploy *Adaptive Response* mitigations is limited. Similarly, many of the deployed solutions may need to be very lean, this reduces the opportunity for *Analytic Monitoring, Dynamic Representation* and *Redundancy*. While the cyber resiliency techniques mentioned here will be useful, in these cases, they will primarily be leveraging what is already in the environment and so are not optimized for the defender goals of reducing and eliminating attacks and gaining and sharing information about those attacks. Note that the environment being defended is now the mission system

The approaches within the *Adaptive Response* technique – *Dynamic Reconfiguration, Dynamic Resource Allocation* and *Adaptive Management* are focused on nimbly implementing courses of action to manage risk. These approaches can most effectively be leveraged in the *Operations and Support* phase if they have been designed into the environment and used with the *Technical Defense-in-Depth* approach of the *Coordinated Defense* technique. The combined techniques provide the defenders with the ability to adaptively respond to attacks this enables the defenders to recover from attacks more effectively and faster than would otherwise be possible. The use of these approaches depends on the flexibility of the operational environment and so these approaches are not usually successful unless planning for them has started early in the design.

5.4 Method for Applying Cyber Resiliency Mitigations and Worked Example

Cyber resiliency enables the operational mission and supporting systems to better anticipate, withstand, recover, and evolve despite adversary attacks and other adverse effects. Thus, when applying supply chain cyber resiliency mitigations to a mission system acquisition, the mitigations ought to be contextualized by, and support, the operational mission. The most effective way for a mission system to achieve maximal cyber resiliency is to start with the "to-be" operational system and work backwards through the acquisitions lifecycle. For each acquisitions phase, these are the appropriate questions that should be asked:

- **Which supply chain threats pose the largest mission risk?**
  Instead of focusing solely on the mission criticality of assets, we want to apply a broader approach that acknowledges that an adversary is likely to exploit the easiest attack vectors to achieve their objective. To do this we want to identify which threats pose the most risk to the mission – those threats that are the most likely and may cause the most harm to the overall mission.

- **How might the mission system be improved to mitigate the most damaging supply chain attacks or compromises?**

If some of the supply chain attacks will be successful, we want to assure the mission system and the supply chain against those that pose the largest risk.

- **How might we improve the recovery & evolution of the system against future supply chain threats?**
  Mitigating existing and known threats is a good start to protect against the latest supply chain threats. However, the adversaries will continue to evolve new tactics and techniques that take advantage of new technologies. Adopting flexible design and engineering decisions will help operators and system engineers better support and defend the system throughout its operational sustainment.

For each acquistion phase these three questions and a sample set of answers are listed below to demonstrate how to apply this mindset to develp mitiations using the Multi-level Domain Campus WLAN Capability and attacks (Section 1, Figure 4).

5.4.1 *Operations and Support*

In the *Operations & Support* phase, the full mission system, including our WLAN capability is deployed and fully operational. The system is being actively used by users and is under attack by adversaries. The major supply chain threats come from changes to the system by way of configuration changes, security patches, feature additions, and technology refresh cycles. At this point, there are no changes to the tech baseline and the supply chain adversary should have sufficient knowledge of the architecture, including hardware and software vendors, versions, and configurations.

Table 3 contains sample answers to the question of which supply chain threats pose the biggest mission risks during the *Operations and Support* phase.

Table 3. Supply Chain Threats and the Associated Mission Risks (*Operations and Support)*

Supply Chain Threat	Mission Risk
Modified configurations and software	Management Services, Authentication Services impacts mission risk across confidentiality, integrity, and availability vectors
Compromised end user wireless devices and VPN client software	Large integrity and confidentiality risk for the domains and data they are permitted to access
Modified configurations and software	Red-side IPS/IDS impacts mission risk across confidentiality and availability
Modified configurations or software on the VPN Gateway	Mission confidentiality (using less secure channels) and availability
Modifications to configurations and firmware/software for grey-side Network, Gateway, and Firewall devices	Mission availability
Limited updates to firmware and hardware threat likelihood	Minor impact on mission risk

Table 4 contains sample answers to the question of how to improve the mission system to mitigate the most damaging supply chain attacks and compromises during the *Operations and Support* phase.

Table 4. Mitigating the Impact of Supply Chain Attacks and Compromises on the Mission System ***(Operations and Support)***

Cyber Resiliency Technique	Application
Substantiated Integrity	Preserve the integrity and provenance of the configuration and software to mitigate most of the risk
Substantiated Integrity in combination with Privilege Restriction	Adopt two-person configuration change authority. Implement processes to require at least two different user authorizations before software and configuration changes become operational
Substantiated Integrity in combination with configuration and change management solutions	Leverage triple entry accounting [19] approaches to provide integrity-assured change management. Approaches include blockchain and certain distributed version management, which can be combined with digital signatures to provide a cryptographically tamperproof chain of custody for soft assets
Substantiated Integrity in combination with Redundancy	Version control assets as virtual machine (VM) images. Do change management over the entire asset as a VM, multiple versions of a VM can be simultaneously supported, allowing for staged, incremental rollouts as well as efficient rollback to minimize impacts from malicious supply chain injects or substitutions
Substantiated Integrity in combination with Realignment	Tailor V&V efforts. Identify unique and comprehensive functional and operational verification & validation (V&V) approaches specific for the mission system and perform testing before deploying anything to production. Every mission system should have a testing facility that can accurately simulate operational conditions. Tests should examine functionality, minimizing updates' impact on integrity or availability, as well as the baseline performance, and aiding in counterfeit identification. By policy, all new and modified hardware, firmware, software, or configuration changes should be thoroughly tested in such a facility before being approved for operational use
Segmentation	Isolate software execution. Segment the OS from the hardware and firmware through virtualization and hypervisors. Use application containers or other execution sandboxes to contain execution impact and minimize the ability for supply chain implants to establish and maintain footholds
Privilege Restriction:	Constrain Resource Usage. Placing limits on software resource usage limits an adversary's effectiveness as well as the overall adverse impact a software supply chain implant could have
Diversity	Consider alternatives to traditional security patching. If an attacker can infiltrate an upstream software vendor, their biggest challenge becomes how to move the compromised software into the target environment. Leveraging security patching is one method. Instead of immediately applying new security patches, consider the need for the patch and potential alternative methods for detection and mitigation (e.g., disabling noncritical features, IDS/IPS signatures)

Analytic Monitoring	Monitor performance. While the *Operation & Sustainment* phase is late for adapting design or improving mission system flexibility, supply chain implants will consume some resources and affect performance or data integrity. By monitoring historical performance characteristics across resources, certain types of implants may be detectable (e.g., grey market, time bombs)
Coordinated Defense	Adopt proven SCRM controls. Follow supply chain risk management [5] and physical protection [20] guidance to sustain provenance integrity and decrease chances of compromise during operations

Table 5 provides sample answers to the question of how to improve the recovery of and evolve the capability of the mission system against future supply chain attacks during the *Operations and Support* phase.

Table 5. Improving Recovery and Evolution of the Capability Against Future Supply Chain Threats *(Operations and Support)*

Cyber Resiliency Technique	Application
Adaptive Response, Dynamic Representation	Monitor (supply chain) threat landscape. Continually monitor the threat landscape and update processes, detection, and countermeasures for potential adverse supply chain tactics, techniques, and protocols (TTPs) against current or potential vendors and suppliers as well as similar technologies or components, which may be applied against current or future supply chain channels
Realignment	Take advantage of refresh and Plan of Action and Milestones (POA&M) cycles. Minor improvements can be made through technology refresh cycles and similar point upgrades by migrating towards products that support common industry standards, allowing for future flexibility

5.4.2 Production and Deployment

During the *Production & Development* phase, the mission system architecture has been finalized and the various hardware and software components are being mass produced per specifications. The components are being delivered to the organization and being integrated and tested to ensure the composite system meets functionality and operational requirements. A supply chain adversary could tamper with the production and delivery, potentially injecting or modifying components. This is the adversary's opportune time to compromise commercial (non-custom) hardware.

Table 6 contains sample answers to the question of which supply chain threats pose the biggest mission risks during the *Production and Deployment* phase.

Table 6. Supply Chain Threats and the Associated Mission Risks *(Production and Deployment)*

Supply Chain Threat	Mission Risk
Modified software for Management Services, and Authentication Services	Risks across confidentiality, integrity, and availability vectors
Compromised end user wireless devices and VPN client software	Large integrity and confidentiality risk for the domains and data they are permitted to access

Modified software to the red-side IPS/IDS	Compromises mission confidentiality and availability
Modified software on the VPN Gateway	Compromises mission confidentiality (using less secure channels) and availability
Modified grey-side Network, Gateway, and Firewall hardware, firmware, and software	Risk mission availability
Configuration is not a concern as that is done primarily during integration at the start of the O&S phase	N/A

Table 7 contains sample answers to the question of how to improve the mission system to mitigate the most damaging supply chain attacks and compromises during the *Production and Deployment* phase.

Table 7. Mitigating the Impact of Supply Chain Attacks and Compromises on the Mission System *(Production and Deployment)*

Cyber Resiliency Technique	Application
Substantiated Integrity	Preserve the integrity and provenance of the software to mitigate most of the highest risks.
Substantiated Integrity in combination with Diversity	Use digital signatures with verified authorities to sign software and firmware updates
Substantiated Integrity in combination with Analytic Monitoring	Perform functional and operational verification & validation (V&V) testing. Some issues, such as VPN tunnels using weaker encryption or exposing side channels, are detectable through monitoring and baselining during the V&V processes
Coordinated Defense	Follow supply chain risk management guidance [5] to sustain provenance integrity and decrease chances of compromise during production and delivery (e.g., blind buys and tamper evident packaging)

Table 8 provides sample answers to the question of how to improve the recovery of and evolve the capability of the mission system against future supply chain attacks during the *Production and Deployment* phase.

Table 8. Improving Recovery and Evolution of the Capability Against Future Supply Chain Threats *(Production and Deployment)*

Cyber Resiliency Technique	Application
Adaptive Response, Dynamic Representation	Continually monitor the supply chain threat landscape. Update processes and monitoring to detect potential threats and tactics against current or potential vendors, suppliers and similar technologies or components, which may be applied against current or future supply chain channels
Diversity	Maintain up-to-date lists of alternative suppliers to enable rapid re-purchases of equipment if supply chain issues are identified with the primary supplier
Redundancy	Identify other organizations with similar capabilities and components to provide an option to use or borrow equipment in cases of supply chain corruption

5.4.3 Engineering and Manufacturing

Earlier phases of the acquisitions lifecycle shift the focus from materiel assets to data assets, including mission system architecture, design, and development documents and specifications. Changes made to these softer components will have an impact on the actual design and production of the final components.

It is during the *Engineering and Manufacturing Development* phase that the custom system components are functionally specified, designed, built, and initially tested. In our example, the WLAN CSfC is developed using commercial solutions, so we do not have to worry about the supply chain threats to customized or unique component development. If we did have such a component, it would most likely be a critical component and be at the top of the list as having the largest mission risk. Therefore, our example will focus largely on preserving the integrity of the engineering and design decisions, rather than new capability development.

Table 9 contains sample answers to the question of which supply chain threats pose the biggest mission risks during the *Engineering and Manufacturing* phase.

Table 9. Supply Chain Threats and the Associated Mission Risks (*Engineering and Manufacturing*)

Supply Chain Threat	Mission Risk
Modified hardware, firmware, and software designs and components for critical components	Risks across confidentiality, integrity, and availability vectors
WLAN CSfC developed from commercially available solutions for hardware, firmware and software	Minor Risk - Adversaries would have a hard time targeting a specific organization and would have to compromise the product across its entire user base, increasing the likelihood of detection

Table 10 contains sample answers to the question of how to improve the mission system to mitigate the most damaging supply chain attacks and compromises during the *Engineering and Manufacturing* phase.

Table 10. Mitigating the Impact of Supply Chain Attacks and Compromises on the Mission System (*Engineering and Manufacturing*)

Cyber Resiliency Technique	Application
Substantiated Integrity	Preserve the integrity and provenance of data assets (e.g., documentation, design, firmware, software).
Substantiated Integrity in combination with Redundancy	Use distributed version control. Encourage contractors and vendors to use distributed, triple entry accounting [21] approaches to provide integrity-assured version management, which can be combined with digital signatures to provide a cryptographically tamper proof chain of custody for soft assets
Dynamic Positioning, Diversity	Give preference to individual components over integrated solutions. Stovepipe engineering and manufacturing efforts enables the acquisition to compartmentalize knowledge, making it harder for the adversary to understand and compromise the entire mission system design. For example, the WLAN acquisition may prefer to purchase the WLAN controller and wireless access points from different vendors rather than as a package

Diversity	Use distributed processing across multiple hardware platforms. Distributed processing decouples the command execution from the specific operational data flow. Distributing the processing, makes it difficult for an adversary to precisely target a specific capability or algorithm through supply chain hardware modification. Additionally, the redundancy requires an adversary to compromise exponentially more systems to increase operational impact
Redundancy	Use redundant processing paths for critical capabilities. Compare the results of critical, repeatable and consistent algorithms across multiple runs on multiple platforms. By performing a calculation multiple times with the same input, it is easy to spot discrepancies in the results, indicating a potential loss of supply chain integrity

Table 11 provides sample answers to the question of how to improve the recovery of and evolve the capability of the mission system against future supply chain attacks during the *Engineering and Manufacturing* phase.

Table 11. Improving Recovery and Evolution of the Capability Against Future Supply Chain Threats (Engineering and Manufacturing)

Cyber Resiliency Technique	Application
Adaptive Response	Adopt industry standards. The use of industry standards and supporting products can accelerate recovery and system evolution through the promotion of standardized capabilities and communications. This allows products to be more easily switched to ones with less supply chain risk, without major impact to the system. These standards usually come with a larger user community and vendor interoperability testing, providing additional levels of supply chain mitigations and assurances. In the WLAN CP, this could mean leverage standard authentication protocols (e.g., Extensible Authentication Protocol (EAP), 802.1X, Kerberos), IPSec VPNs, and Information Technology Infrastructure Library (ITIL) or ISO/IEC 20000 compatible management frameworks.
Dynamic Positioning	Prefer swappable components. Some components are more easily replaced with alternatives. For example, the WLAN wireless access points are probably easy to change. Similarly, most software can be run on a variety of hardware platforms, which can be quickly swapped in case of a supply chain threat. There are also swappable hardware components, such as disk drives and other chassis.
Diversity	Evaluate potential hardware and software alternatives. If a supply chain threat is realized, a standby list of potential alternatives will improve recovery speed. For higher risk, higher threat environments, it may be beneficial to perform and maintain some level of regular functionality and integration testing for one or two alternatives during sustainment

5.4.4 *Technology Development & Materiel Solutions Analysis*

The earliest, pre-systems acquisition phases are primarily focused on data and documents, namely requirements and metrics such as key performance parameters (KPPs) and key system attributes (KSAs). This focus limits the number of people, organizations, and technologies, significantly limiting the attack vectors available to supply chain adversaries. However, any successful attacks could have far reaching implications through all subsequence acquisitions phases, including *Operations & Sustainment*.

Table 12 contains sample answers to the question of which supply chain threats pose the biggest mission risks during the *Technology Development* and *Materiel Solutions Analysis* phases

Table 12. Supply Chain Threats and the Associated Mission Risks (Technology Development and Materiel Solutions Analysis)

Supply Chain Threat	Mission Risk
Modified requirements document can lessen the robustness, security, and resiliency of the overall mission system and any custom components	can reduce the robustness, security, and resiliency of the overall mission system and any custom components

Table 13 contains sample answers to the question of how to improve the mission system to mitigate the most damaging supply chain attacks and compromises during the *Technology Development* and *Materiel Solutions Analysis* phase.

Table 13. Mitigating the Impact of Supply Chain Attacks and Compromises on the Mission System (Technology Development and Materiel Solutions Analysis)

Cyber Resiliency Technique	Application
Substantiated Integrity	Preserve the integrity and provenance of documentation and related requirements for both mission system and contractor performance.
Substantiated Integrity in combination with Redundancy	Use distributed version control. Encourage contractors and vendors to use and audit integrity-assured version management, which can be combined with digital signatures to provide a cryptographically tamperproof chain of custody for soft assets
Substantiated Integrity in combination with Diversity	Diversify development. Develop documents and requirements using a variety of applications and formats. This minimizes the impacts that an adversary can have by targeting a single document or application. For example, requirements writing may use a combination of word processing, system engineering, and spreadsheet tools from different vendors. An adversary would have to make corresponding changes to each different document to avoid detection
Substantiated Integrity in combination with Realignment	Prefer simpler formats. Contrary to diversifying development, many applications use custom binary or complex file formats. These formats make it difficult to determine and audit changes across versions, and synchronize revisions across documents. By using simpler, text based formats, acquisitions teams can focus on specific requirements and maintain a clean provenance trail

Substantiated Integrity in combination with Privilege Restriction	Minimize write access. Limit the number of users with the authority to make changes to the official versions of the documents and designs
Segmentation	Segment development efforts. Stovepipe pre-system acquisition development efforts and compartmentalize knowledge, making it harder for the adversary to understand and impact the overall mission system development and requirements

Table 14 provides sample answers to the question of how to improve the recovery of and evolve the capability of the mission system against future supply chain attacks during the *Technology Development* and *Materiel Solutions Analysis* phase.

Table 14. Improving Recovery and Evolution of the Capability Against Future Supply Chain Threats (Technology Development and Materiel Solutions Analysis

Cyber Resiliency Technique	Application
Realignment, Adaptive Response	Adopt a composable system architecture. Design the mission system using technologies that provide future flexibility, such as virtualization, software-defined networking (SDN), and other dynamic representation approaches. The ability to change and adapt the system will make it easier to mitigate later supply chain threats, as well as improve later engineering and operational flexibility
Segmentation	Own the data interfaces. Design the system around data services using service-oriented architecture (SOA) concepts. The organization should own and specify the critical data interfaces. By owning these interfaces, an organization can better define, monitor, and secure the channel (e.g., read/write privileges, cross-domain validation), while increasing the ability to switch out the components behind the interface

This page intentionally left blank.

6 Next Steps

This report has presented a general analysis approach for applying cyber resiliency techniques and approaches to the acquisition lifecycle. It focuses on demonstrating how the adversary uses the CAL over the entire acquisition life cycle and the impact on the *Operations and Support* phase of the acquisition life cycle. The cyber resiliency mitigations are those that can be applied to reduce or eliminate impacts to the operational end mission system.

We have also demonstrated that the CAL is recursive and each stage of the acquisition life cycle and those systems used within that phase are a target for an adversary.

We identify systems and system environments within the acquisition lifecycle that an adversary might target in planning and executing supply chain attacks. Next, we associate the adversary goals with respect to the stages of the cyber attack lifecycle against these systems and system environments keeping in mind that the adversary's end goal is to impact the mission. We identify which cyber resiliency techniques – and which approaches to implementing or applying those techniques – might be effective in preventing the adversary from achieving this goal.

Systems security engineers can use the analysis presented in this report as a starting point for program-specific refinement, enabling development and execution of a Program Protection Plans (PPP) that addresses cyber supply chain risks effectively. Program-specific refinement of the general analysis presented in this report needs to take into consideration such programmatic constraints as reliance on legacy components, components of uncertain provenance, or shared services. SSEs supporting a Program Office will be able to evaluate how well the Program Office (and its ICT support), the Prime or Integration Contractor, and other organizations (e.g., the Maintenance Contractor if different from the Prime, IV&V, cyber range) are applying cyber resiliency throughout the acquisition lifecycle to reduce supply chain risks due to cyber attacks.

To apply these recommendations, Programs will need to include requirements motivated by cyber resiliency into contractual documents, specifically SOWs and FRDs. SOW requirements will lead to contractors (the Prime or Integration Contractor, the Maintenance Contractor if different, and subcontractors as appropriate) applying selected cyber resiliency techniques in the design, production, test, and maintenance environments, to make the supply chain more cyber resilient. FRD requirements will make acquired mission systems more resilient against cyber attacks that exploit weaknesses in the supply chain.

Next steps could include development of detailed notional worked examples, with sample contractual language; extending the analysis beyond the focus on ICT to include weapons systems or platform IT (PIT); and application to a specific mission system.

This page intentionally left blank.

Appendix A References

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

[2] 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 Technique," The MITRE Corporation, Bedford, MA, 2015.

[3] M. Reed, J. F. Miller and P. Popick, "Supply Chain Attack Patterns: Framework and Catalog," 2014. [Online]. Available: http://www.acq.osd.mil/se/docs/Supply-Chain-WP.pdf.

[4] Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD/AT&L), "Department of Defense Instruction 5000.02," 7 January 2015. [Online]. Available: http://www.acq.osd.mil/fo/docs/500002p.pdf.

[5] J. Boyens, C. Paulsen, R. Moorthy and N. Bartol, "NIST Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations," April 2015. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-161.

[6] DoD Defense Science Board, "DSB Task Force Report on Cyber Supply Chain," February 2017. [Online]. Available: https://www.hsdl.org/?view&did=799509.

[7] D. o. D. D. C. (AT&L), "Defense Technical Information Center," 25 August 2016. [Online]. Available: http://www.esd.whs.mil/portals/54/documents/DD/issuances/dodi/520044p.pdf. [Accessed 10 July 2017].

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

[9] D. Bodeau and R. Graubart, "Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment," February 2014. [Online]. Available: http://www.mitre.org/publications/technical-papers/characterizing-effects-on-the-cyber-adversary-a-vocabulary-for.

[10] ODNI, "Cyber Threat Framework," [Online]. Available: https://www.dni.gov/index.php/cyber-threat-framework.

[11] National Institute of Standards and Technology, "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.

[12] Office of the DASD (DT&E), "Guidelines for Cybersecurity DT&E, version 1.0," 19 April 2013. [Online].

[13] 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.

[14] Cisco TALOS , "New Ransomeware Varient "Nyeta" compromises systems Worldwide," 27 June 2017. [Online]. Available: http://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html (still under investigation). [Accessed 7 July 2017].

[15] NSA Information Assurance Directorate (IAD), "Campus Wireless Local Area Network Capability Package," 27 April 2016. [Online]. Available: https://www.nsa.gov/resources/everyone/csfc/capability-packages/assets/files/campus-wlan-cp.pdf.

[16] R. Graubart and D. Bodeau, "The Risk Management Framework and Cyber Resiliency," The MITRE Corporation, McLean, VA, 2016.

[17] R. Ross, M. McEvilley and J. C. Oren, "NIST SP 800-160 System Security Engineering: Considerations for a Multidisplinary Approach in the Engineering of Trustworthy Secure Systems," May 2016. [Online]. Available: http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf. [Accessed 21 June 2017].

[18] J. F. Miller, "Supply Chain Attack Framework and Attack Patterns," 2013. [Online]. Available: https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf.

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

[20] I. Grigg, "Triple Entry Accounting," 25 December 2005. [Online]. Available: http://iang.org/papers/triple_entry.html.

[21] The MITRE Corporation , "Common Attack Pattern Enumeration and Classification," 9 January 2017. [Online]. Available: https://capec/mitre.org/data/. [Accessed 31 August 2017].

[22] National Institute of Standards and Technology, "NIST Special Publication 800-37rev1: Guide for Applyuing the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," February 2010. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/sp800-37-rev1-final.pdf.

[23] NIST, Computer Security Division, Information Technology Laboratory, "NIST Special Publications," February 2004. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf. [Accessed 11 July 2017].

[24] DoD, "DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle, Version 1.0," 26 May 2015. [Online].

[25] SCRM Program Management Office (PMO) Globalization Task Force (GTF) OASD(NII)-CIO/ODASD(CIIA), "Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11 Supply Chain Risk management Pilot Program," 2010.

[26] National Institute of Standards and Technology, "NIST Special Publication 800-30rl: Guide for Conducting Risk Assessments," September 2012. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30rl.pdf.

[27] The Open Group, "Open Trusted Technology Provider Standard (O-TTPS), Version 1.1," July 2014. [Online]. Available: https://www2.opengroup.org/ogsys/catalog/c147. [Accessed 11 July 2017].

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

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

[30] USD(AT&L), "Directive-type Memorandum (DTM) 17-001 – Cybersecurity in the Defense Acquisition System," 11 January 2017. [Online]. Available: https://www.hsdl.org/?view&did=797977.

[31] 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.

This page intentionally left blank.

Appendix B Analysis of Known Supply Chain Attacks

In August, 2014, the Office of the Deputy Assistant Secretary of Defense for Systems Engineering (DASD-SE) described 41 known supply chain attacks [3]. Subsequently, the "Common Attack Pattern Enumeration and Classification [22]" was updated to include these 41 attacks. In the DASD-SE paper, each attack is characterized by:

- Target (hardware, software, firmware or system information)
- Description
- Vector (path followed by attacker)
- Origin (e.g., insider, outsider)
- Goal (Disruption, Corruption, Disclosure, Destruction)
- Impact
- References
- Threat
- Vulnerabilities exploited
- Attack Points within the Supply Chain
- Applicable Acquisition Life Cycle Phases

It is important to note that the "target" for these 41 supply chain attacks are predominetly ICT components. An "attack" within the DASD-SE paper is the successful insertion, modification or substitution[13] to/of a component within the supply chain (regardless of whether or not it makes it into an operational system.) In this paper, the DASD-SE "attacks" are referred to as attack "steps" that are taken to complete a full cyber-attack on the end mission or system, using the Cyber Attack life-cycle. These steps (or actions) are mapped to the stages in the cyber attack lifecycle described in Section 2.4, using the following definitions and rationale:

- Reconnaissance — the adversary develops a target; Example: Gathering information about components used in the end mission system
- Weaponize — the attack is put in a form to be executed on the victim's computer/network;Example: An piece of software is modified during the development stage
- Deliver—the vulnerability is delivered to the target; Example: the modified software is offered and accepted as a patch
- Exploit — the initial attack on target is executed;Example: The modified software is on the end system and ready to execute
- Control—mechanisms are employed to manage the initial victims; Example: The adversary has a way into receive and manage the results from the successful exploit
- Execute — leveraging numerous techniques, the adversary executes the plan; and
- Maintain — long-term access is achieved.

To better understand the adversary's objectives in using the supply chain to exploit a targeted network and end mission system, we have analyzed the 41 defined supply chain attacks steps

[13] The categories of insertion modification and substitution were created to combine information included in the goal, impact, threat and vulnerabilities descriptions in the DASDE-SE paper.

[19] by grouping them by methods used: Insertion, Substitution, or Modification. These methods are used by an adversary to achieve their goals working across the acquisition life cycle with the focus on impacting an end mission system in the *Operations and Support* phase.

These attack method types are defined as follows:

- Insertion: Adding additional information, code, or functionality to an ICT module or component which performs a new, malicious function or otherwise subverts the intended system functions. For example, adding malicious code to a software library. Most attacks of this type are applicable to systems under development.
- Substitution: A complete replacement of a module or component (hardware, software, firmware) to be integrated into the system with one that has already been tampered with in order to maliciously change its intended function or operation.
- Modification: Any change of existing design or other information that defines the system under development. In most cases, the change will be to cause a degradation or weakness in later development or production.

The intent of this analysis is to understand and characterize the adversary's goals within the acquisition life cycle. This analysis does not represent the frequency of actual attack steps, but instead groups the 41 attack steps in relation to the acquisition lifecycle to observe trends in the occurrence of the attack steps and relate them to the adversary's goals.

The breakdown of substitution attack steps across the acquisition life cycle (Figure 6, below), shows that they occur in both the *Engineering & Manufacturing Development* (15 attack steps) and *Production & Deployment (14 attack steps) phases* nearly equally. Eleven of those attack steps occur in <u>both</u> the *Engineering and Manufacturing Development* and *Production and Deployment* phases. Access to a component supplier is usually a prerequisite for performing a substitution attack step. Understanding the adversary's goal of substituting hardware in the *Engineering & Manufacturing Development*, *Production & Deployment* and *Operations and Support* phases of the acquisition life cycle, means that resiliency mitigations should be focused on hardware integrity and tracking. For an operational network, it can be assumed that some hardware has been compromised. Software as a substitution attack frequently occurs during the *Operations and Support* phase of the acquisition life cycle as software products are maintained.

Insertion can be directed at software, hardware, firmware or information. The number of attack stepss characterized as insertion (9 attack steps) is smaller than substitution attack steps (24 attack steps).

It is important to note that many of the 41 attacks cited in the sources require some knowledge of the system under development, the suppliers, the development and production environments, etc. If access to information is properly controlled, adversarial reconnaissance can be curtailed.

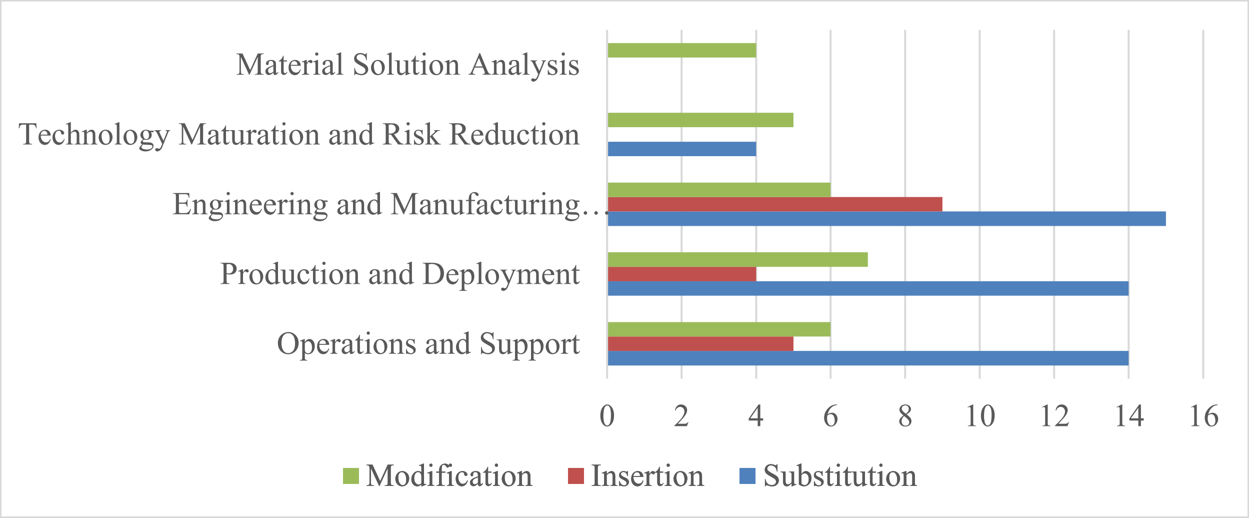

Figure 6. Supply Chain attack steps within the Acquisiton Lifecycle

This page intentionally left blank.

Appendix C Analysis of Applicable Existing Supply Chain Risk Management Guidance

The SCRM controls described in existing guidance and the resiliency mitigations proposed in this report complement each other as discussed below. Both should be used by SSEs. Below are the National Institute for Standards and Technology (NIST) documents reviewed for this task:

- NIST Special Publication (SP) 800-161 "Supply Chain Risk Management Practices for Federal Information Systems and Organizations" [5]. This document is a supply chain risk management overlay for NIST SP 800-53 R4 [20].
- NIST SP 800-30, Revision 1, "Guide for Conducting Risk Assessments" [12]
- NIST SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework (RMF) to Federal Information Systems" [23]
- NIST Federal Information Processing Standard (FIPS)199, "Standards for Security Categorization of Federal Information and Information Systems," [24]

When conducting a risk assessment in accordance with the DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle [24], using NIST SP 800-161 and NIST SP 800-30R10R1, an SSE works with their customer to assess risk at the mission and information system level. The recommendations of resiliency mitigations in Section 5 of this paper will guide the SSE to include cyber resiliency as one method of risk mitigation. Table 15 below summarizes the activities an SSE performs when conducting a risk assessment and the complementary activities performed as part of a cyber resiliency analysis. For a discussion of how cyber resiliency relates to the RMF, see the MITRE white paper "The Risk Management Framework and Cyber Resiliency" [17].

Table 15. Cyber Resiliency Activities Compared to Risk Management Framework Activities

Risk Management Framework Activities for Assessing Risk	Cyber Resiliency Analysis Activities
Criticality Analysis	Determine Mission essential cyber resources and cyber resiliency objectives
Analyze Threats and Known Vulnerabilities	Analyze adversary capabilities, intent and targeting
Determine likelihood of a threat exploiting a vulnerability	Address inherent weaknesses in mission/business processes, weaknesses in information security, architecture and cyber defense processes.
Determine impact to system/mission	Determine impact with a focus on Consequence to Mission
Accept, Mitigate, Share, Transfer or Avoid Risk	Mitigate Adversary TTPs via cyber resiliency techniques Ensure mission and system can anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources

The document "Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11 Supply Chain Risk Management Pilot Program "provides 32 key practices for managing supply chain risks throughout a system design lifecycle [26]. It focuses on practices that enable the development and operation of systems to meet their cost, schedule and performance requirements within a globalized market and with active adversaries. The audience is system engineers, program managers, government prime contractors and subcontractors and those responsible for delivery and supporting systems with supply chain assurance.

We analyzed the key practices against cyber resiliency techniques and discovered where the key practice supports cyber resiliency, is a part of cyber resiliency, has no overlap or is a complete overlap with cyber resiliency. There are four key practices that overlap with cyber resiliency techniques:

Table 16. Key Practices Guidance and Its Relation to Cyber Resiliency

Key Practice	Cyber Resiliency Technique
KP8 Protect Critical Elements and Processes	Cyber resiliency technique selection driven by mission/business objectives, environment architecture and threat environment
KP 9 Use defensive Design	Cyber resiliency technique selection driven by mission/business objectives, environment architecture and threat environment
KP 10 Use/Create standard interfaces to increase supplier diversity	Part of the Diversity technique
KP19 Perform Penetration Testing	Activities in this practice are part of Coordinated Defense Technique

The key practices guide is a good source document for SSEs but focuses on recommendations for program managers and acquisition specialists.

Appendix D Summary of Cyber Resiliency Techniques and Approaches

Table 17 summarizes cyber resiliency techniques and the rationale for applying them (i.e., the objective an organization using it expects to achieve).

Table 17. Cyber Resiliency Techniques

Cyber Resiliency Technique	Rationale
Adaptive Response: Implement nimble cyber courses of action to manage risks	Optimize the organization's ability to respond in a timely and appropriate manner to adverse conditions, stresses, or attacks, thus maximizing the ability to maintain mission operations, limit consequences, and avoid destabilization.
Analytic Monitoring: Gather, fuse, and analyze data on an ongoing basis and in a coordinated way to identify potential vulnerabilities, adverse conditions, stresses, or attacks, and damage	Maximize the organization's 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 cyber situational awareness.
Coordinated Defense: Manage multiple, distinct mechanisms in a non-disruptive or complementary way	Ensure that failure of a single defensive barrier does not expose critical assets to threat exposure. Require threat events to overcome multiple safeguards; in the case of adversarial events, this makes it more difficult for the adversary to successfully attack critical resources, increasing the cost to the adversary, and raising the likelihood of adversary detection. Ensure that uses of any given defensive mechanism do not create adverse unintended consequences by interfering with other defensive mechanisms.
Deception: Mislead, confuse, or hide critical assets from the adversary	Mislead or confuse the adversary, or hide critical assets from the adversary, making them uncertain how to proceed, delaying the effect of their attack, increasing the risk to them of being discovered, causing them to misdirect or waste their attack and expose their tradecraft prematurely.
Diversity: Use heterogeneity to minimize common mode failures, particularly attacks exploiting common vulnerabilities	Limit the possibility of a collapse of critical functions due to failure of replicated common components. In the case of adversarial threats, cause the adversary to work harder by developing malware or other Tactics, Techniques, and Procedures (TTPs) appropriate for multiple targets, increase the chance that the adversary will waste or expose TTPs by applying them to targets for which they are inappropriate, and maximize the chance that some of the defending organization's system's will survive the adversary's attack.
Dynamic Positioning: Distribute and dynamically relocate functionality or assets	Increase the ability of an organization to rapidly recover from non-adversarial events (e.g., fires). Impede an adversary's ability to locate, eliminate or corrupt mission/business assets, and cause the adversary to spend more time and effort to find the organization's critical assets, thereby increasing the chance of the adversary revealing their actions and tradecraft prematurely.

Cyber Resiliency Technique	Rationale
Dynamic Representation: Construct and maintain current representations of mission posture in light of cyber events and cyber courses of action	Support situational awareness, enhance understanding dependencies among cyber and non-cyber resources, reveal patterns/trends in adversary behavior; and validate the realism of courses of action.
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 advance and potentially expunging an adversary's foothold from in the system.
Privilege Restriction: Restrict privileges required to use cyber resources, and privileges assigned to users and cyber entities, based on the type(s) and degree(s) of criticality	Limit the impact and probability that unintended actions by authorized individuals will compromise information or services. Impede the 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 cyber resources with core aspects of mission/business functions	Minimize the connections between mission critical and non-critical services, thus reducing likelihood that a failure of non-critical services will impact mission critical services. Reduce the attack surface of the defending organization by minimizing the chance that non-mission/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/Isolation: Define and separate (logically or physically) components based on criticality and trustworthiness	Contain adversary activities and non-adversarial stresses (e.g., fires) to the enclave/segment in which they have established a presence; for adversarial cyber activities, this limits the number of possible targets to which malware can easily be propagated.
Substantiated Integrity: Ascertain whether critical services, information stores, information streams, and components 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; provide limited capabilities for repair.
Unpredictability: Make changes randomly or unpredictable	Increase the adversary's uncertainty regarding the cyber defenses that they may encounter, thus making it more difficult for them to ascertain the appropriate course of action.

Cyber resiliency "approaches" are specific ways to implement cyber resiliency techniques. For the above resiliency techniques, the Cyber Resiliency Engineering Framework (CREF) [2] defines 44 representative approaches to implementing those techniques. Table 18 provides the CREF definitions for selected resiliency approaches.

Table 18. Definitions of Cyber Resiliency Approaches

Cyber Resiliency Technique	Cyber Resiliency Approach	Definition
Adaptive Response	Dynamic Reconfiguration	Make changes to an element or component while it continues operating.
	Dynamic Resource Allocation	Change the allocation of resources to tasks or functions without terminating critical functions or processes.
	Adaptive Management	Change how defensive mechanisms are used based on changes in the operational environment as well as changes in the threat environment.
Analytic Monitoring	Monitoring and Damage Assessment	Monitor and analyze behavior and characteristics of components and resources to look for indicators of adversary activity, detect and assess damage, and watch for adversary activities during recovery and evolution.
	Sensor Fusion and Analysis	Fuse and analyze monitoring data and preliminary analysis results from different components, together with externally provided threat intelligence.
	Malware and Forensic Analysis	Analyze malware and other artifacts left behind by adversary activities.
Coordinated Defense	Technical Defense-in-Depth	Use multiple protective mechanisms at different architectural layers or locations.
	Coordination and Consistency Analysis	Apply processes, supported by analytic tools, to ensure that defenses are applied and cyber courses of action are defined and executed in a coordinated, consistent way that minimizes interference.
Deception	Obfuscation	Hide, transform, or otherwise obfuscate information from the adversary.
	Dissimulation/ Disinformation	Provide deliberately misleading information to adversaries.
	Misdirection/ Simulation	Maintain deception resources or environments and direct adversary activities there.
Diversity	Architectural Diversity	Use multiple sets of technical standards, different technologies, and different architectural patterns.
	Design Diversity	Use different designs to meet the same requirements or provide equivalent functionality.
	Synthetic Diversity	Transform implementations to produce a variety of instances.
	Information Diversity	Provide information from different sources or transform information in different ways.

Cyber Resiliency Technique	Cyber Resiliency Approach	Definition
	Command, Control, and Communication Path Diversity	Provide multiple paths, with demonstrable degrees of independence, for information to flow between components.
	Supply Chain Diversity	Use multiple, demonstrably independent, supply chains for critical components.
Dynamic Positioning	Functional Relocation of Sensors	Relocate sensors, or reallocate responsibility for specific sensing tasks, to look for indicators of adversary activity, and to watch for adversary activities during recovery and evolution.
	Functional Relocation of Cyber Assets	Change the location of assets that provide functionality (e.g., services, applications) or information (e.g., data stores), either by moving the assets or by transferring functional responsibility.
	Asset Mobility	Physically relocate physical assets (e.g., platforms or vehicles, mobile computing devices).
	Distributed Functionality	Distribute functionality (e.g., processing, storage, and communications) across multiple components.
Dynamic Representation	Dynamic Mapping & Profiling	Maintain current information about resources, their status, and their connectivity.
	Dynamic Threat Modeling	Maintain current information about threat activities and characteristics (e.g., observables, indicators, TTPs).
	Mission Dependency & Status Visualization	Maintain current information about mission dependencies on resources, and the status of those resources with respect to threats.
	Non-Persistent Information	Refresh information periodically, or generate information on demand, and delete the information when no longer needed.
Non-Persistence	Non-Persistent Information	Refresh information periodically, or generate information on demand, and delete the information when no longer needed.
	Non-Persistent Services	Refresh services periodically, or generate services on demand and terminate services after completion of a request.
	Non-Persistent Connectivity	Establish connections on demand, and terminate connections after completion of a request or after a period of non-use.
Privilege Restriction	Privilege Management	Define, assign, and maintain privileges associated with end users and cyber entities, based on established trust criteria, consistent with principles of least privilege.
	Privilege-Based Usage Restrictions	Define, assign, maintain and apply usage restrictions on cyber resources based on mission criticality and other attributes.
	Dynamic Privileges	Elevate or deprecate privileges assigned to a user, process, or service based on transient or contextual factors.

Cyber Resiliency Technique	Cyber Resiliency Approach	Definition
Realignment	Purposing	Ensure cyber resources are used consistent with critical mission purposes.
	Offloading/ Outsourcing	Offload supportive but non-essential functions to a service provider that is better able to support the functions.
	Restriction	Remove or disable unneeded risky functionality or connectivity, or add mechanisms to reduce the risk.
	Replacement	Replace risky implementations with less-risky implementations.
Redundancy	Protected Backup and Restore	Back up information and software (including configuration data) in a way that protects its confidentiality, integrity, and authenticity, and to restore it in case of disruption or destruction.
	Surplus Capacity	Maintain extra capacity for information storage, processing, and/or communications.
	Replication	Duplicate information and/or functionality in multiple locations and keep it synchronized.
Segmentation	Predefined Segmentation	Define and separate components on the basis of criticality and trustworthiness.
	Dynamic Segmentation/ Isolation	Change the definition of enclaves or protected segments, or isolate resources, while minimizing operational disruption.
Substantiated Integrity	Integrity/Quality Checks	Apply and validate checks of the integrity or quality of information, components, or services.
	Provenance Tracking	Identify and track the provenance of data, software, and/or hardware elements.
	Behavior Validation	Validate the behavior of a system, service, or device against defined or emergent criteria.
Unpredictability	Temporal Unpredictability	Change behavior or state at times that are determined randomly or by complex functions.
	Contextual Unpredictability	Change behavior or state in ways that are determined randomly or by complex functions.

This page intentionally left blank.

Appendix E Cyber Resiliency Mitigations Applied to the Acquisition Lifecycle

Based on the effects of cyber resiliency techniques in the cyber attack lifecycle (table 6 of the Engineering Aid) and the cyber resiliency approaches and their specific effects (tables 7-20 of the Engineering Aid [2]; Table H-6 of [18]) we developed the following tables.

It is important to note that because we are applying the CAL to an adversary using the entire acquisition lifecycle with the objective of exploiting the end mission system some of the approaches had slightly different effects than described in the tables referenced because those references assumed a single environment rather than a sequential environment such as acquisition life cycle. These tables are a starting point and should be tailored based on the specific environments and concerns.

Table 19. Cyber Resiliency Mitigations for Materiel Solutions Analysis Phase

Acquisition Lifecycle	Resiliency Mitigations	Adversary Goals (per the CAL)							Defender Goals in O&S			
		Acquire Info	Develop tools	Deliver Attack	Initial Exploit	Controlling attack	Executing Attack	Maintain Presence	Reduce attacks	Limit attack	Gain/Share Info	Recover
Materiel Solutions Analysis	**Deception**											
	Obfuscation – make identifying and targeting high value information resources difficult	**x**							**x**			
	Dissimulation/disinformation – provide the adversary with false information so the attacks developed are ineffective in *Operations and Support*	**x**							**x**	**x**		
	Misdirection – reduce attacks by wasting adversary resources	**x**							**x**	**x**	**x**	
	Non-Persistence											
	Non-Persistent Information – Reduce availability of information on system needs and development	**x**							**x**	**x**		
	Non-Persistent Services – Reduce the chance the adversary has corrupted services in the environment to gain information	**x**							**x**	**x**		
	Non-Persistent Connectivity – reduce means to get information on system needs and developments	**x**							**x**	**x**		
	Privilege Restriction											
	Privilege Management – reduce the number of resources accessible with individual credentials causing the adversary to invest more time and effort	**x**							**x**	**x**		
	Privilege-Based Usage Restrictions – cause the adversary to expend more time and effort to get credentials	**x**							**x**	**x**		
	Dynamic Privileges – increase the difficulty for the adversary in gaining credentials	**x**							**x**	**x**		
	Realignment											
	Restriction – reduce the paths (via risky functionality or connectivity) used by adversaries	**x**							**x**	**x**		
	Segmentation/Isolation											
	Predefined Segmentation – reduces adversary's ability to exfiltrate and the amount of data that can be exfiltrated – limiting the amount of information they can gain	**x**							**x**	**x**		

	Dynamic Segmentation/Isolation – contains adversary activities (e.g., the insertion of malware in running processes and control of compromised processes) limiting how they can gain information	**x**							**x**	**x**		
	Unpredictability											
	Temporal Unpredictability – combine with Dynamic Privileges – increase the difficulty for the adversary in gaining credentials	**x**							**x**	**x**		

Table 20. Cyber Resiliency Mitigations for Technology Maturity and Risk Reduction Phase

Acquisition Lifecycle	Resiliency Mitigations	Adversary Goals (per the CAL)							Defender Goals in O&S			
		Acquire Info	Develop tools	Deliver Attack	Initial Exploit	Controlling attack	Executing Attack	Maintain Presence	Reduce attacks	Limit attack	Gain/Share Info	Recover
Technology Development	**Deception**											
	Obfuscation – make identifying and targeting high value information resources difficult	x							x			
	Dissimulation/disinformation – provide the adversary with false information so the attacks developed are ineffective in *Operations and Support*	x							x	x		
	Misdirection – reduce attacks by wasting adversary resources	x							x	x	x	
	Non-Persistence											
	Non-Persistent Information – limit the adversary's ability to gain information by limiting the time the information is available	x							x	x		
	Non-Persistent Services – limit the amount of time the adversary can exploit a service	x							x	x		
	Non-Persistent Connectivity – limit the amount of time paths into the environment are available	x							x	x		
	Privilege Restriction											
	Privilege Management – reduce the number of resources accessible with individual resources causing the adversary to invest more time and effort	x							x	x		
	Privilege-Based Usage Restrictions – cause adversary to use more time and effort to get credentials	x							x	x		
	Dynamic Privileges – increase the difficulty for the adversary in gaining credentials	x							x	x		
	Realignment											
	Restriction – reduce the paths (via risky functionality or connectivity) used by adversaries	x							x	x		
	Segmentation											
	Predefined Segmentation – reduces adversary's ability to exfiltrate and the amount of data that can be exfiltrated – limiting the amount of information they can gain	x							x	x		
	Dynamic Segmentation/Isolation – contains adversary activities (e.g., the insertion of malware in running processes and control of compromised processes) limiting how they can gain information	x							x	x		

	Unpredictability											
	Temporal Unpredictability – combine with Dynamic Privileges – increase the difficulty for the adversary in gaining credentials	**x**							**x**	**x**		

Table 21. Cyber Resiliency Mitigations for Engineering and Manufacturing Development Phase

Acquisition Lifecycle	Resiliency Mitigations	Adversary Goals (per the CAL)							Defender Goals in O&S			
		Acquire Info	Develop tools	Deliver Attack	Initial Exploit	Controlling attack	Executing Attack	Maintain Presence	Reduce attacks	Limit attack	Gain/Share Info	Recover
Engineering and Manufacturing Development	**Analytic Monitoring**											
	Sensor Fusion and Analysis – exposes adversary activity allowing defenders to gain information about the adversary attacks and share them with later Acquisition lifecycle phases				x	x					x	x
	Malware and Forensic Analysis – analyze adversary activities and artifacts left behind			x	x	x					x	x
	Deception											
	Dissimulation/disinformation – provide the adversary with false information so the attacks developed are detected in this phase or the next, or are less effective in O&S	x	x		x	x			x	x		
	Misdirection – diverting attacks to a honeynet environment, enables defenders to analyze attack TTPs for future defense, eliminates attacks in this phase before they are passed to the next Acquisition lifecycle, and provides information about adversary targets	x	x	x	x	x			x	x	x	x
	Diversity											
	Architectural Diversity/Heterogeneity – adversary must use more time and effort to develop tools that work across diverse implementations and initial exploit may not be as effective	x	x		x				x	x		
	Design Diversity/Heterogeneity – adversary must use more time and effort to develop tools that work across diverse implementations and initial exploit may not be as effective	x	x		x				x	x		
	Supply chain diversity – adversary must use more time and effort to compromise more supply chains or accept that only be a subset of target components will be compromised	x		x					x	x		
	Non-persistence											
	Non-Persistent Information – limit the adversary's ability to deliver an attack, decrease the probability of the initial exploit being successful and reduce the adversary's ability to control malware by limiting the time information is available	x		x	x	x			x	x		

	Non-Persistent Services – limit the adversary’s ability to deliver an attack, decrease the probability of the initial exploit being successful and reduce the adversary’s ability to control malware by limiting the amount of time the adversary can exploit a service	**x**		**x**	**x**	**x**			**x**	**x**		
	Non-Persistent Connectivity – limit the adversary’s ability to deliver an attack, decrease the probability of the initial exploit being successful and reduce the adversary’s ability to control malware by limiting the amount of time paths into the environment are available	**x**		**x**	**x**	**x**			**x**	**x**		
	Privilege Restriction											
	Privilege Management – cause the adversary to expend more time and effort to get credentials to control the malware.	**x**				**x**				**x**		
	Privilege-Based Usage Restrictions – cause the adversary to expend more time and effort to get credentials to control the malware. The initial exploit may also fail due to lack of credentials.	**x**			**x**	**x**				**x**		
	Dynamic Privileges – increase the difficulty for the adversary in gaining credentials	**x**			**x**	**x**				**x**		
	Redundancy											
	Protected Backup and Restore – reduce threat of backups being corrupted by adversary and used as a way into the environment or to maintain a presence			**x**	**x**			**x**	**x**			
	Segmentation											
	Predefined Segmentation – reduces adversary’s ability to deliver and propagate and control malware	**x**		**x**	**x**	**x**			**x**			
	Dynamic Segmentation/Isolation – contains the adversary’s activities (such as the insertion of malware in running processes and control of compromised processes) limiting deliver and propagate and control malware	**x**		**x**	**x**	**x**			**x**			
	Substantiated Integrity											
	Integrity Quality checks – detect the presence of compromised components and remove them from the environment reducing the number of exploits and possibility of information exfiltration			**x**					**x**	**x**	**x**	
	Provenance Tracking – detect the adversary’s attempts to deliver compromised components and remove them from the environment			**x**					**x**	**x**	**x**	
	Behavior Validation – Identify the presence of compromised component in the environment				**x**	**x**			**x**	**x**	**x**	
	Unpredictability											
	Temporal Unpredictability combined with non-persistence – increase the difficulty for the adversary in to deliver malware, initiate the exploit and gain enough control to impact O&S	**x**			**x**				**x**			
	Temporal Unpredictability – combine with Dynamic Privileges – increase the difficulty for the adversary in gaining credentials	**x**		**x**	**x**	**x**			**x**			

	Contextual unpredictability combined with integrity quality checks – make it more difficult for the adversary to emulate components and get compromised components into fielded system			**x**					**x**			

Table 22 . Cyber Resiliency Mitigations for Production and Deployment Phase

Acquisition Lifecycle	Resiliency Mitigations	Adversary Goals (per the CAL)							Defender Goals in O&S			
		Acquire Info	Develop tools	Deliver Attack	Initial Exploit	Controlling attack	Executing Attack	Maintain Presence	Reduce attacks	Limit attack	Gain/Share Info	Recover
Production and Deployment	**Analytic Monitoring**											
	Monitoring and Damage Assessment – Defenders obtain indications and warnings of adversary activities to share later in the Acquisition Lifecycle			x		x		x			x	
	Sensor Fusion and analysis – exposes adversary activity allowing defenders to gain information about the adversary attacks and share them with later Acquisition lifecycle phases					x		x			x	
	Malware and Forensic Analysis – provide the defenders with the adversary's TTPs and capabilities			x	x	x		x			x	
	Coordinated Defense											
	Technical Defense-in-Depth – degrades the attackers' ability to initiate, control, execute or maintain attacks because they must develop attacks against multiple defensive technologies deployed concurrently				x	x	x	x	x	x		x
	Coordination and Consistency Analysis – reduce the attackers' ability to use unintended consequences or unforeseen dependences to disruptions to initiate exploits					x	x	x		x		x
	Deception											
	Dissimulation/disinformation – provide the adversary with false information so the attacks developed are ineffective in O&S					x	x	x	x	x	x	
	Misdirection – diverting attacks to a honeynet environment, enables defenders to analyze attack TTPs for future defense, eliminates attacks in this phase before they are passed to the next Acquisition lifecycle, and provides information about adversary targets				x	x	x	x	x	x	x	x
	Diversity											
	Architectural Diversity/Heterogeneity – adversary must use more time and effort to develop tools that work across diverse implementations and initial exploit may not be as effective		x		x	x	x	x		x		x

	Design Diversity/Heterogeneity – adversary must use more time and effort to develop tools that work across diverse implementations and initial exploit may not be as effective		**x**		**x**	**x**	**x**	**x**		**x**		**x**
	Command, Control and Communications Path Diversity – increase the defender's ability to remove attackers by using uncompromised communications channels once defenders become aware of exploit							**x**		**x**		
	Supply chain diversity – adversary must use more time and effort to compromise more supply chains or accept that there will only be a subset of target components compromised			**x**	**x**					**x**		
	Dynamic Positioning											
	Functional Relocation of Sensors – increase the likelihood of detecting adversary by tailoring sensor location this also makes it harder for the adversary to maintain their presence					**x**	**x**	**x**		**x**	**x**	
	Distributed Functionality – increase the number of elements the adversary must compromise to deny or corrupt functionality					**x**		**x**		**x**		
	Dynamic Representation											
	Dynamic Mapping and Profiling – identify software and components that do not conform to policy requirements or that are behaving in unexpected ways					**x**		**x**			**x**	
	Dynamic Threat Modeling – reveal patterns and trends in adversary behaviors to share with O&S phase					**x**		**x**			**x**	
	Mission Dependency and Status Visualization – identify consequences of adversary execution to share with O&S phase						**x**				**x**	
	Non-persistence											
	Non-Persistent Information – limit the adversary's presence from delivery through maintenance by limiting the time information is available			**x**	**x**	**x**	**x**	**x**	**x**	**x**		
	Non-Persistent Services – limit the adversary's presence from delivery through maintenance by limiting the time the adversary can exploit a service			**x**	**x**	**x**	**x**	**x**	**x**	**x**		
	Non-Persistent Connectivity – limit the adversary's presence from delivery through maintenance by limiting the time paths into the environment are available			**x**	**x**	**x**	**x**	**x**	**x**	**x**		
	Privilege Restriction											
	Privilege Management – cause the adversary to expend more time and effort to get credentials to deliver, initiate, control and execute the attack as well as maintain their presence			**x**	**x**	**x**	**x**	**x**	**x**	**x**		
	Privilege-Based Usage Restrictions – cause the adversary to expend more time and effort to get credentials to do anything in the environment			**x**	**x**	**x**	**x**	**x**	**x**	**x**		
	Dynamic Privileges – increase the difficulty for the adversary in gaining credentials			**x**	**x**	**x**	**x**	**x**		**x**		

	Redundancy											
	Protected Backup and Restore - reduce threat of backups being corrupted							**x**	**x**			
	Segmentation											
	Predefined Segmentation – reduces adversary’s ability to initiate exploit, control the malware, execute attacks and maintain their presence				**x**	**x**	**x**	**x**	**x**			
	Dynamic Segmentation/Isolation – contains the adversary’s activities (such as the insertion of malware in running processes and control of compromised processes) limiting the adversary’s ability to initiate exploit, control the malware, execute attacks and maintain their presence				**x**	**x**	**x**	**x**	**x**			
	Substantiated Integrity											
	Integrity Quality checks – detect the presence of compromised components and remove them from the environment reducing the number of exploits and possibility of information exfiltration			**x**					**x**			
	Provenance Tracking – detect the adversary’s attempts to deliver compromised components and remove them from the environment			**x**					**x**			
	Behavior Validation – Identify the presence of compromised component in the environment				**x**	**x**	**x**	**x**	**x**	**x**		
	Unpredictability											
	Temporal Unpredictability combined with non-persistence – increase the difficulty for the adversary in to deliver malware, initiate the exploit and gain enough control to impact O&S			**x**	**x**	**x**	**x**	**x**	**x**	**x**		
	Temporal Unpredictability – combine with Dynamic Privileges – increase the difficulty for the adversary in gaining credentials			**x**	**x**	**x**	**x**	**x**	**x**	**x**		
	Contextual unpredictability combined with integrity quality checks – make it more difficult for the adversary to emulate components and get compromised components into fielded system				**x**			**x**	**x**			

Table 23. Cyber Resiliency Mitigations for Operations and Support Phase

Acquisition Lifecycle	Resiliency Mitigations	Adversary Goals (per the CAL)							Defender Goals in O&S			
		Acquire Info	Develop Tools	Deliver Attack	Initial Exploit	Control Attack	Executing Attack	Maintain	Reduce attacks	Limit Attack	Gain/Share Info	Recover
Operations and Support	**Adaptive Response**											
	Dynamic Reconfiguration – making configuration changes during operations makes it harder for the adversary to control malware limiting the success of attacks					**x**	**x**	**x**		**x**		**x**
	Dynamic Resource Allocation – changes the resources available for the adversary to exploit					**x**	**x**	**x**		**x**		**x**
	Adaptive Management – changing how defensive mechanisms are used based on changes in the operational environment or threat environment forces the adversary to continue adapting to changes in the environment					**x**	**x**	**x**		**x**		**x**
	Analytic Monitoring											
	Monitoring and Damage Assessment – Defenders obtain indications and warnings of adversary activities to share						**x**	**x**			**x**	
	Sensor Fusion and analysis – exposes adversary activity allowing defenders to gain information about the adversary attacks						**x**	**x**			**x**	
	Malware and Forensic Analysis – provide the defenders with the adversary's TTPs and capabilities						**x**	**x**			**x**	
	Coordinated Defense											
	Technical Defense-in-Depth – degrades the attackers' ability to initiate, control, execute or maintain attacks because they must develop attacks against multiple defensive technologies deployed concurrently					**x**	**x**	**x**		**x**		**x**
	Coordination and Consistency Analysis – reduce the attackers' ability to use unintended consequences or unforeseen dependences to disruptions to initiate exploits					**x**	**x**	**x**		**x**		**x**
	Diversity											
	Architectural Diversity/Heterogeneity – adversary must use more time and effort to develop tools that work across diverse implementations – attacks may not be as effective						**x**			**x**		**x**

	Design Diversity/Heterogeneity – adversary must use more time and effort to develop tools that work across diverse implementations and attacks may not be as effective						x			x		x
	Command, Control and Communications Path Diversity – increase the defender's ability to remove attackers by using uncompromised communications channels once they become aware of exploit							x		x		x
	Supply chain diversity – adversary must use more time and effort to compromise more supply chains or accept that there will only be a subset of target components compromised						x			x		
	Dynamic Positioning											
	Functional Relocation of Sensors – increase the likelihood of detecting adversary by tailoring sensor location this makes it harder for the adversary to maintain their presence					x	x	x		x	x	
	Distributed Functionality – increase the number of elements the adversary must compromise to deny or corrupt functionality						x	x		x		x
	Dynamic Representation											
	Dynamic Mapping and Profiling – identify software and components that do not conform to policy requirements or that are behaving in unexpected ways							x		x	x	
	Dynamic Threat Modeling – reveal patterns and trends in adversary behaviors							x			x	
	Mission Dependency and Status Visualization – identify consequences of adversary execution										x	x
	Non-persistence											
	Non-Persistent Information – limit the adversary's presence throughout the CAL by limiting the time information is available					x	x	x	x	x		x
	Non-Persistent Services – limit the adversary's presence throughout the CAL by limiting the time the adversary can exploit a service					x	x	x	x	x		
	Non-Persistent Connectivity – – limit the adversary's presence throughout the CAL by limiting the time paths into the environment are available					x	x	x		x		
	Privilege Restriction											
	Privilege Management – cause the adversary to expend more time and effort to get credentials to control and execute the attack as well as maintain their presence					x	x	x	x	x		
	Privilege-Based Usage Restrictions – cause the adversary to expend more time and effort to get credentials					x	x	x		x		
	Dynamic Privileges – increase the difficulty for the adversary in gaining credentials					x	x	x		x		
	Redundancy											

	Protected Backup and Restore - reduce threat of backups being corrupted							x		x		x
	Segmentation											
	Predefined Segmentation – reduces adversary’s ability to control the malware, execute attacks and maintain their presence					x	x	x		x		
	Dynamic Segmentation/Isolation – contains the adversary’s activities (such as the manipulation of malware in running processes and control of compromised processes) limiting the adversary’s ability to control the malware, execute attacks and maintain their presence					x	x	x		x		x
	Substantiated Integrity											
	Integrity Quality checks – detect the presence of compromised components and remove them from the environment reducing the number of exploits and possibility of information exfiltration						x		x		x	
	Provenance Tracking – detect the adversary’s attempts to deliver compromised components and remove them from the environment			x			x		x		x	
	Behavior Validation – Identify the presence of compromised component in the environment							x		x	x	x
	Unpredictability											
	Temporal Unpredictability combined with non-persistence – increase the difficulty for the adversary in to gain control of the fielded system					x	x	x		x		
	Temporal Unpredictability – combine with Dynamic Privileges – increase the difficulty for the adversary in gaining credentials					x	x	x		x		
	Contextual unpredictability combined with integrity quality checks – make it more difficult for the adversary to emulate components and get compromised components into fielded system					x	x	x	x	x		

Appendix F Abbreviations and Acronyms

AMT	Active Management System
BIOS	Basic Input Output System
C2	Command and Control
CAL	Cyber Attack Lifecycle
CAPEC	Common Attack Pattern Enumeration and Classification
CDD	Capability Development Document
CIA	Confidentiality, Integrity and Availability
COTS	Computer off-the-shelf
CP	Capability Package
CREF	Cyber Resiliency Engineering Framework
CSfC	Commercial Solutions for Classified
CTF	Cyber Threat Framework
DASD-SE	Deputy Assistant Secretary of Defense/Systems Engineering
DIMFUI	Degradation, Interruption, Modification, Usurption and Interception
DLL	Dynamic-Link Library
DoD	Department of Defense
DSB	Defense Science Board
DT&E	Developmental Test and Evaluation
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standard
FRD	Functional Requirements Document
ICD	Initial Capabilities Document
ICT	Information and Communications Technology
IDS	Intrusion Detections System
IEC	International Electrotechnical Commission
IPS	Intrusion Prevention System
ISO	International Organization for Standards
ITIL	Information Technology Infrastructure Library
KPP	Key Performance Parameters
KSA	Key System Attributes

LAN	Local Area Network
LMS	Local Manageability Service
NIST	National Institute for Standards and Technology
OS	Operating System
O-TTPS	Open Trusted Technology Provider Standard
PIT	Platform IT
POA&M	Plan of Action and Milestones
POET	Political, Operational, Economic and Technical
RMF	Risk Management Framework
SCRM	Supply Chain Risk Management
SDN	Software Defined Network
SOA	Service Oriented Architecture
SOW	Statement of Work
SSE	System Security Engineer
TMRR	Technology Maturation and Risk Reduction
TTP	Tactics Techniques and Procedures
UEFI	Unified Extensible Firmware Interface
V&V	Verification and Validation
VM	Virtual Machine
VPN	Virtual Private Network
WLAN	Wireless LAN