Carnegie Mellon University
Software Engineering Institute

Acquisition Security Framework (ASF): Managing Systems Cybersecurity Risk

Christopher Alberts
Michael Bandor
Charles M. Wallen
Carol Woody

October 2022

TECHNICAL NOTE

CMU/SEI-2022-TN-003

DOI: 10.1184/R1/21357627

CERT Division

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

http://www.sei.cmu.edu

Copyright 2022 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

This report was prepared for the SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

CERT® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM22-1065

Table of Contents

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

List of Figures

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Abstract

The Acquisition Security Framework (ASF) is a collection of leading practices for building and operating secure and resilient software-reliant systems across the systems lifecycle. It enables programs to evaluate risks and gaps in their processes for acquiring, engineering, and deploying secure software-reliant systems and provides programs more insight and control over their supply chains. The ASF provides a roadmap for building security and resilience into a system rather than "bolting them on" after deployment. The framework is designed to help programs coordinate the management of engineering and supply chain risks across the many components of a system, including hardware, network interfaces, software interfaces, and mission capabilities. ASF practices promote proactive dialogue across all program and supplier teams, helping to integrate communications channels and facilitate information sharing. The framework is consistent with cybersecurity engineering, supply chain management, and risk management guidance from the International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), and Department of Homeland Security (DHS). This report presents an overview of the ASF and its development status. It also includes a snapshot of the practices that have been developed so far and outlines a plan for completing the ASF body of work.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

1 Introduction

The Acquisition Security Framework (ASF) is a collection of leading practices for building and operating secure and resilient software-reliant systems. The ASF is designed to enable systems security and resilience engineering across the lifecycle and supply chain. It provides a roadmap for building security and resilience into a system rather than "bolting them on" after deployment. The ASF documents leading practices and provides a pathway for proactive process management. This dual focus on practices and processes produces an efficient and predictable acquisition and development environment, which ultimately leads to reduced security and resilience risks in deployed systems.

Software is a growing component of modern business and mission-critical systems. As organizations become more dependent on software-driven technology, security and resilience risks to their missions also increase, largely due to increased complexity and external dependencies. Management of these risks is too often deferred until after deployment due to competing priorities, such as meeting cost and schedule objectives. However, experience shows that failure to address these risks early in the systems lifecycle increases mitigation costs and severely limits mitigation options.

Today's growing reliance on third-party suppliers to help achieve cost and schedule objectives introduces supply chain risks that are inherited by the systems being put in place. As a result, program leaders and engineering personnel must manage these inherited risks across the systems lifecycle. The ASF is structured to help programs manage inherited and other avoidable risks by identifying options to implement a proactive stance from the earliest point in the systems lifecycle. Effective management of supply chain risk requires integrating multiple processes that foster effective collaboration across the range of stakeholders responsible for acquiring, developing, and deploying software-reliant systems.

Many security and resilience solutions focus on a few aspects of engineering, such as security requirements specification, secure coding practices, or supply chain risk management. In contrast, the ASF leverages a proven set of integrated program management, engineering, and supplier management practices and processes that span the systems lifecycle. ASF practices promote proactive dialogue across all program and supplier teams, helping integrate communications channels and facilitate information sharing. As a result, the ASF enables programs to acquire, develop, and operate complex software-reliant systems that function at lower risk in an increasingly contested, challenging, and interconnected cyber environment.

1.1 The Evolving Role of Software and Suppliers

Software assurance is defined as a level of confidence that software will function as intended and will be free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software, throughout the acquisition lifecycle [NIA 2010]. Software assurance was legislatively mandated for the Department of Defense (DoD) in the "National Defense Authorization Act

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

for Fiscal Year 2013" [U.S. Code 2013]. The pursuit of software assurance is a worthy goal that must be translated into practical methods that acquirers, engineers, designers, and developers can apply throughout the acquisition lifecycle.

Software assurance is becoming increasingly important to organizations across all sectors because of software's increasing influence in business- and mission-critical systems. For example, consider how the size of flight software has increased over the years. Between 1960 and 2000, the degree of functionality provided by software to the pilots of military aircraft has increased from 8% to 80%. At the same time, the size of software in military aircraft has grown from 1,000 lines of code in the F-4A to 1.7 million lines of code in the F-22. This trend is expected to continue over time [Dvorak 2009]. As software exerts more control over complex systems, like military aircraft, the potential risk posed by cybersecurity vulnerabilities will increase in kind.

Cost is another dimension of cybersecurity vulnerabilities that must be considered. Many cybersecurity vulnerabilities are software faults because their root causes can be traced to the software's requirements, architecture, design, or code. Studies have shown that the cost of addressing a software fault increases significantly (up to 200 times) if it is corrected during operations as opposed to design [Mainstay 2010, Microsoft 2014, Soo Hoo 2001]. In addition, rework related to defects consumes more than 50% of the effort associated with a software project. Therefore, it is more cost effective to address software faults early in the acquisition lifecycle rather than to wait until operations. This principle applies to many operational security vulnerabilities as well. Figure 1 illustrates the concept of addressing security practices across the lifecycle.

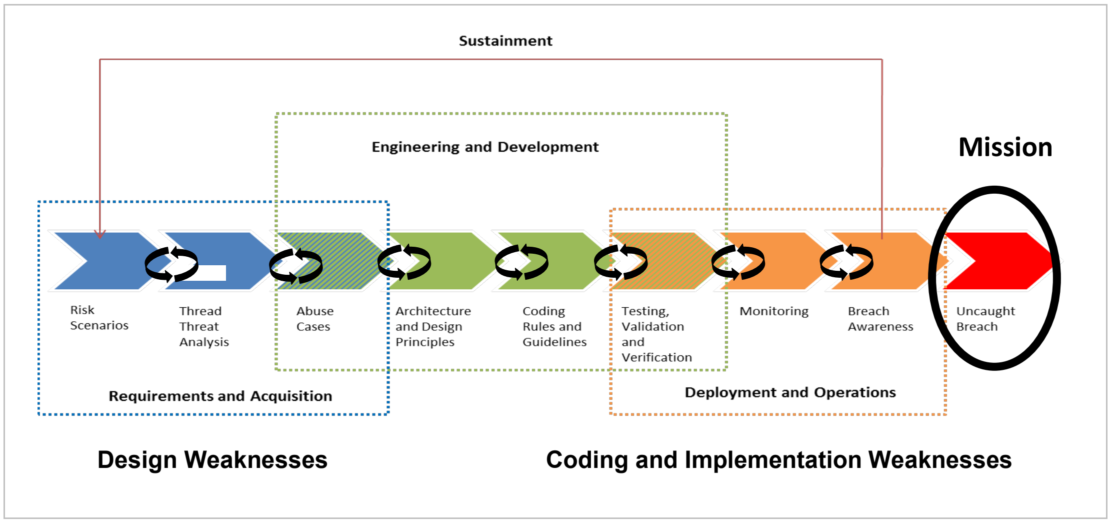
Sustainment
Engineering and Development
Mission
Risk Scenarios
Thread Threat Analysis
Abuse Cases
Architecture and Design Principles
Coding Rules and Guidelines
Testing, Validation and Verification
Monitoring
Breach Awareness
Uncaught Breach
Requirements and Acquisition
Deployment and Operations
Design Weaknesses
Coding and Implementation Weaknesses

Figure 1: Cybersecurity Practices Available Across the Lifecycle to Address Security Weaknesses

Operational security vulnerabilities generally have three main causes: (1) design weaknesses, (2) implementation/coding errors, and (3) system configuration errors. Addressing design weaknesses as soon as possible is especially important because these weaknesses are not easy to correct after a system has been deployed. For example, software maintenance organizations normally cannot issue a patch to correct a fundamental security issue related to the software's requirements, architecture, or design. Remediation of design weaknesses normally requires extensive changes to the system; these changes can be costly and often prove to be impractical for the implemented

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

system. As a result, software-reliant systems with design weaknesses often are allowed to operate under a higher degree of residual security risk, putting their associated operational missions in jeopardy.

At the SEI, our field experience indicates that few acquisition and development programs currently implement effective cybersecurity engineering practices. These programs have historically emphasized meeting performance, cost, and schedule objectives over meeting security and resilience objectives. In addition, the traditional focus on implementing operational controls to achieve compliance does not address the supplier's increasingly important role in providing components, products, and services to acquisition programs.

In our previous cybersecurity engineering research and development, we focused on documenting systems and software security and resilience practices across the acquisition and development lifecycle [Alberts 2017a]. These practices are essential for reducing the potential success of cyber attacks. This focus on engineering practices addresses a key aspect of cyber risk management. A second important area to consider is third-party and supplier management. As programs increasingly become reliant on third-party products and services, the supply chain becomes a growing source of cyber risk for those programs. We have observed that few programs implement effective supplier oversight early in the acquisition lifecycle. Our ASF research-and-development work has expanded our engineering focus to include cyber risks introduced by suppliers and other program dependencies.

1.2 Audience

The ASF's focus is on managing the cyber risks associated with software-reliant systems, particularly systems designed to operate in large and complex environments. Ensuring that cyber risk is considered from the earliest aspects of the systems lifecycle makes ASF research uniquely valuable for program managers, acquisition and contracting personnel, project leads, engineering team members, and security personnel. Each of these groups is part of the main audience for the ASF and this report.

Operational security and resilience staff might also find information in this report to be useful. The ASF addresses several deployment and operational issues related to managing security and resilience during operations and sustainment. In addition, we have observed that a program's focus on security and resilience does not end with deployment. The risk-based processes used to engineer and develop resilient software-reliant systems should carry over into operations and sustainment to ensure that security and resilience endure. Operational staff need to have effective processes for updating and refining software-reliant systems to meet the evolving threat landscape and the rapid pace of technology change.

Finally, ASF concepts and practices apply to federal government and private sector groups, such as technology, cybersecurity, the defense industrial base, aerospace, and service providers. The ASF is built around the notion that systems security and resilience require collaboration among many groups across multiple sectors. Personnel from these organizations will also find information in this report to be useful.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

1.3 Report Structure

We present the current research-and-development status for the ASF in this report. Our development of the ASF is a work in progress. This report provides a snapshot of the practice areas that we have developed so far and outlines our plan for completing this body of work. It comprises the following sections and appendices:

- Section 1: Introduction provides a brief introduction to the ASF and some of the motivation for its development.
- Section 2: ASF Lineage presents previous SEI research that we have leveraged when developing the ASF.
- Section 3: ASF Overview describes the ASF's structure and provides summaries of the six ASF practice areas.
- Section 4:Conclusion and Next Steps presents an overview of future research and development that will be performed for developing, codifying, and piloting the ASF.
- Appendix A: ASF Domains, Goals, and Questions presents the domains, goals, and questions (i.e., practices) for four of the six ASF practice areas.
- Appendix B: ASF Glossary provides the definitions of terms related to the ASF and its use.

The main purpose of this report is to present an overview of the ASF and its development status. Before we provide an overview of the framework's structure and content, we first explore the ASF's research and development lineage in the next section.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

2 ASF Lineage

The ASF is built on SEI research in software engineering and cyber risk over the past several decades. Many SEI solutions share a common theme—using technology to enable mission success. This theme has driven the development of several innovative SEI solutions, such as Capability Maturity Model Integration (CMMI), Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), and CERT Resiliency Management Model (CERT-RMM). These solutions resulted in highly influential bodies of knowledge that have informed the subsequent development of many methods, tools, and techniques, including the ASF. However, the ASF's research influences are not limited to CMMI, OCTAVE, and CERT-RMM. As illustrated in Figure 2, the ASF has a rich research lineage.

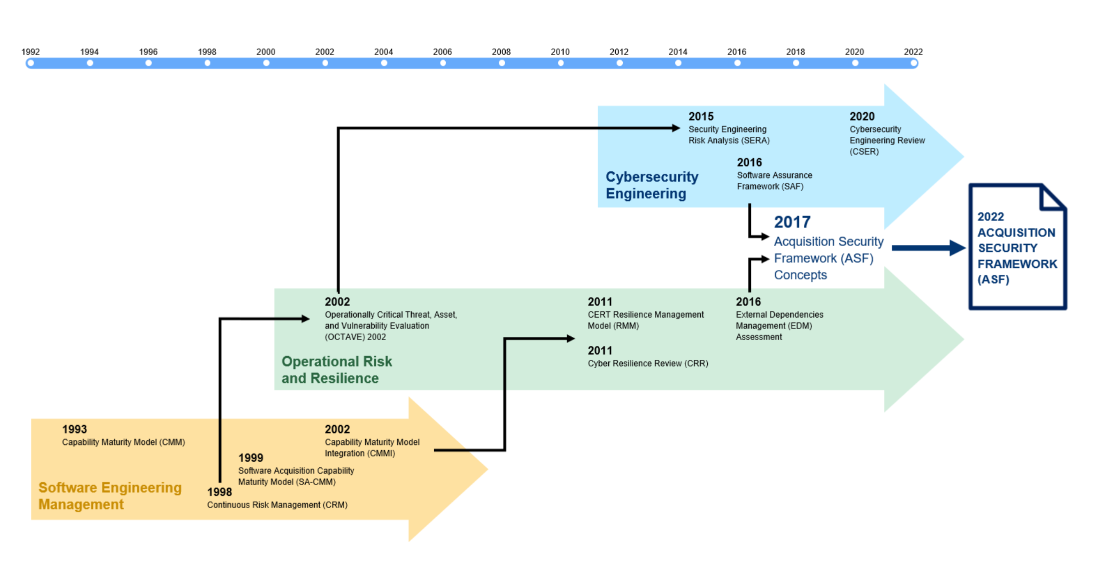
1992
1994
1996
1998
2000
2002
2004
2006
2008
2010
2012
2014
2016
2018
2020
2022
2015
Security Engineering Risk Analysis (SERA)
2020
Cybersecurity Engineering Review (CSER)
2016
Software Assurance Framework (SAF)
Cybersecurity Engineering
2017
Acquisition Security Framework (ASF) Concepts
2022
ACQUISITION SECURITY FRAMEWORK (ASF)
2002
Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) 2002
2011
CERT Resilience Management Model (RMM)
2016
External Dependencies Management (EDM) Assessment
2011
Cyber Resilience Review (CRR)
Operational Risk and Resilience
1993
Capability Maturity Model (CMM)
2002
Capability Maturity Model Integration (CMMI)
1999
Software Acquisition Capability Maturity Model (SA-CMM)
1998
Continuous Risk Management (CRM)
Software Engineering Management

Figure 2: Research Lineage of the ASF

Previous SEI research that influenced ASF development includes the following areas: software engineering management, operational risk and resilience, and cybersecurity engineering. Each of these areas is briefly explored in the following sections.

2.1 Software Engineering Management

The research lineage of the ASF stretches back almost three decades to the development of the Capability Maturity Model (CMM). The CMM is a process maturity framework that was designed to help organizations improve their software development process [Paulk 1993]. This seminal work defined an approach for managing and improving organization processes, which influenced many subsequent solutions. One of those solutions is the Software Acquisition Capability Maturity Model (SA-CMM), which was designed to improve the maturity of software acquisition

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

processes for government and industry organizations [Ferguson 1996]. CMMI was developed to unite the software and acquisition CMMs to create one unified model [Chrissis 2006].

As the CMM and CMMI were being developed, SEI researchers began developing an approach for managing risks during software development. Continuous Risk Management (CRM) describes the underlying principles, concepts, and functions of risk management and provides guidance on how to implement them as a continuous practice in projects and organizations [Dorofee 1996]. CRM provided the paradigm for many subsequent SEI risk management solutions.

2.2 Operational Risk and Resilience

One of the risk management solutions influenced by CRM is OCTAVE, a framework for identifying and managing information security risks [Alberts 2002]. OCTAVE defines a comprehensive evaluation method that allows an organization to identify the information assets that are important to the mission of the organization, the threats to those assets, and the vulnerabilities that may expose those assets to threats. By analyzing information assets, threats, and vulnerabilities, an organization can begin to understand which information assets are at risk. With this understanding, the organization can design and implement a protection strategy that reduces the overall risk exposure of its information assets.

OCTAVE and CMMI were major influences on the development of CERT-RMM, a process improvement model that documents leading practices from industry and government for managing operational resilience [Caralli 2011]. CERT-RMM integrates the following organizational areas: security management, business continuity management, and aspects of information technology (IT) and operations management. Based on the CERT-RMM, the SEI developed the Cyber Resilience Review (CRR) to assess an organization's cyber resilience [DHS 2014]. The CRR establishes a baseline of cybersecurity capabilities that helps an organization understand (1) its operational resilience and (2) its ability to manage cyber risks to critical services during normal operations as well as during times of operational stress and crisis.

Managing supplier-oriented risks was a key factor driving SEI research in operational risk and resilience. The growing complexity of threats required organizations to employ more systematic approaches to cyber risk management across their networks of suppliers. The interconnected nature of cybersecurity among internal and external stakeholders required a more collaborative and integrated management approach. The External Dependencies Management (EDM) Assessment was developed to provide organizations with a risk-based method for managing external dependency and supply chain risks. The EDM Assessment leverages the CRR assessment platform and extends it to evaluate how an organization protects and sustains services and assets that are dependent on the actions of suppliers and other external organizations.

2.3 Cybersecurity Engineering

The SEI's cybersecurity engineering research incorporates many of the concepts and principles from previous work in software engineering management and operational risk and resilience. In 2010, SEI researchers noticed the need for improved cybersecurity engineering early in the lifecycle. At that time, security and resilience solutions were largely focused on operation and sustainment. There was a growing need to develop solutions for building security and resilience into software-reliant systems rather than waiting to address cyber risks during operations.

The SERA Method defines a scenario-based approach for analyzing complex cybersecurity risks in software-reliant systems and systems of systems across the lifecycle and supply chain [Alberts 2014]. SERA integrates CRM's early lifecycle view on risk with OCTAVE's operational view. SERA provides a platform for analyzing risk in systems that are being acquired and developed. While developing the SERA Method, SEI researchers identified a need within the cyber community to establish more effective security and resilience practices across the systems lifecycle.

The Software Assurance Framework (SAF) documents cybersecurity practices that programs can apply across the acquisition lifecycle and supply chain. The SAF can be used to assess an acquisition program's current cybersecurity practices and chart a course for improvement, ultimately reducing the cybersecurity risk of deployed software-reliant systems [Alberts 2017a]. The SAF was influenced by CMMI and CERT-RMM.

When developing the SAF, SEI researchers identified a need to assess programs against SAF practices, leading to the development of the Cybersecurity Engineering Review (CSER). The CSER assesses how well a program integrates cybersecurity into its software and systems engineering practices. The CSER provides a program with a roadmap for integrating security into its practices for acquiring and engineering highly complex software-reliant systems. The CRR and EDM assessments influenced the structure and format of the CSER.

2.4 ASF Development

In 2016, SEI researchers collaborated to create an integrated, systems-oriented approach that considers the entire risk management lifecycle. This was the genesis of the ASF [Alberts 2017b]. ASF research-and-development activities include SEI researchers from multiple disciplines, including cybersecurity engineering, operational risk and resilience, and acquisition.

Managing supply chain cyber risk is especially challenging because it is broad and pervasive, and responsibility is spread widely across multiple organizations. Today's complex threats and organizational structures call for a more systematic approach to managing multiple internal and external stakeholders. This applies not only to daily operations, but also to the acquisition and development of complex systems. Acquisition and development personnel must consider the operational context and implement a plan for managing suppliers' risks across the lifecycle. Operational personnel must establish processes that effectively integrate each supplier into an organization's existing processes and practices.

From a third-party perspective, the ASF documents leading supplier management practices. Here, the goal is to measure and improve an organization's ability to manage third-party cyber risks across the systems lifecycle. The ASF provides a mechanism for increasing an organization's confidence about the level of its suppliers' performance, improving its understanding of potential gaps, and making improvements based on a suggested roadmap.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

From a broader perspective, the ASF defines a process management approach for engineering technology and collaborating with suppliers to deliver and operate complex systems. Initial development of the ASF in 2016 focused on defining key concepts and principles. Current ASF development was initiated in 2020. Our objective is to build on ASF foundational concepts and principles by developing and documenting leading practices for managing security and resilience across the systems lifecycle and supply chain.

The centerpiece of this work is a risk-based framework that enables programs to do the following:

- Manage program security and resilience risks collaboratively across the lifecycle and supply chain.
- Incorporate security and resilience practices that scale to selected acquisition pathways and development approaches.
- Implement an appropriate level of process management and improvement (i.e., maturity) for security and resilience practices.

Acquisition and engineering practices continue to evolve. Emerging threats and increased system complexity have given rise to new process-based techniques that are designed to manage cyber risks from early requirements definition through operations. These new practices have brought improved methods and outcomes, including a lifecycle orientation shared by DevSecOps[1] and the ASF. In the next section, we present the organizing structure of the ASF and provide summaries of the six ASF practice areas.

[1] DevSecOps stands for development, security, and operations. It defines an approach for integrating security as a shared responsibility throughout the software lifecycle, from initial design through integration, testing, deployment, and software delivery. DevSecOps requires a change in culture, process, and tools across development, security, and operations teams, which makes security a shared responsibility across the organization. Automation is a critical component of DevSecOps because it enables process efficiency, allowing developers, infrastructure, and information security teams to focus on delivering value rather than applying manual, error-prone security practices.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

3 ASF Overview

The ASF is a collection of leading security and resilience practices across the lifecycle and supply chain. It enables programs to evaluate risks and gaps in their processes for acquiring, engineering, and deploying secure software-reliant systems and provides programs more insight and control over their supply chains. The ASF is designed to help a program coordinate management of engineering and supply chain risks across the many components of a system, including hardware, network interfaces, software interfaces, and mission capabilities. The SEI's core objective for the ASF is to design a solution that enables programs to plan for and manage the challenges resulting from today's inherently complex acquisition, engineering, and operational environments.

3.1 ASF Challenge Areas

We begin by highlighting three key challenges that the ASF is designed to address.

The first challenge is implementing integrated risk management processes. Managing cyber resilience risks is a continuous process that is performed

- across the lifecycle
- by multiple groups
- from multiple perspectives
- at multiple points in time

As a result, a program must implement cyber risk processes that enable collaboration among multiple stakeholder groups. We have embedded practices for collaborative risk management into the ASF.

The second challenge is integrating security and resilience practices into a program's existing acquisition, engineering, and supplier management practices. Security and resilience management is not a standalone activity that is performed separate from other types of program practices. Programs need to implement security and resilience as a part of their daily technical and management responsibilities. In addition, security and resilience practices need to be flexible and tailorable. They should scale to multiple acquisition pathways; support multiple cyber-focused standards, laws, and regulations; and apply to new development approaches, such as DevSecOps. We developed the ASF with this type of integration and flexibility in mind.

The third challenge is focused on process management and improvement. System qualities, such as security and resilience, are highly influenced by the quality of the processes used to develop and maintain them. Higher degrees of process management produce more stable management environments, leading to more consistent results over time. Effectively managed processes also enable programs and systems to achieve their missions, predictably. The challenge is to implement an appropriate level of process management across a program, helping to ensure that security and resilience risks are managed successfully across the program team and its suppliers. The ASF's risk-based, process management approach addresses this challenge.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

The remainder of this section provides an overview of the ASF's content. First, we describe the ASF's basic architecture and structure. We conclude this section by presenting the six ASF practices areas.

3.2 ASF Structure

Figure 3 shows how the ASF is structured as a multi-layered framework that comprises practice areas, domains, goals, and practices. At the top level, the ASF is organized into six primary practice areas. Each practice area has multiple domains supporting it. A domain is focused on a given technical or management topic, such as program planning, risk management, or requirements. Each domain has multiple goals supporting it. An ASF goal defines the outcome or objective toward which a program's effort is directed. Finally, each ASF goal is supported by a group of practices. Practices describe discrete activities that must be performed to achieve a goal. In this report, ASF practices are phrased as questions.[2]

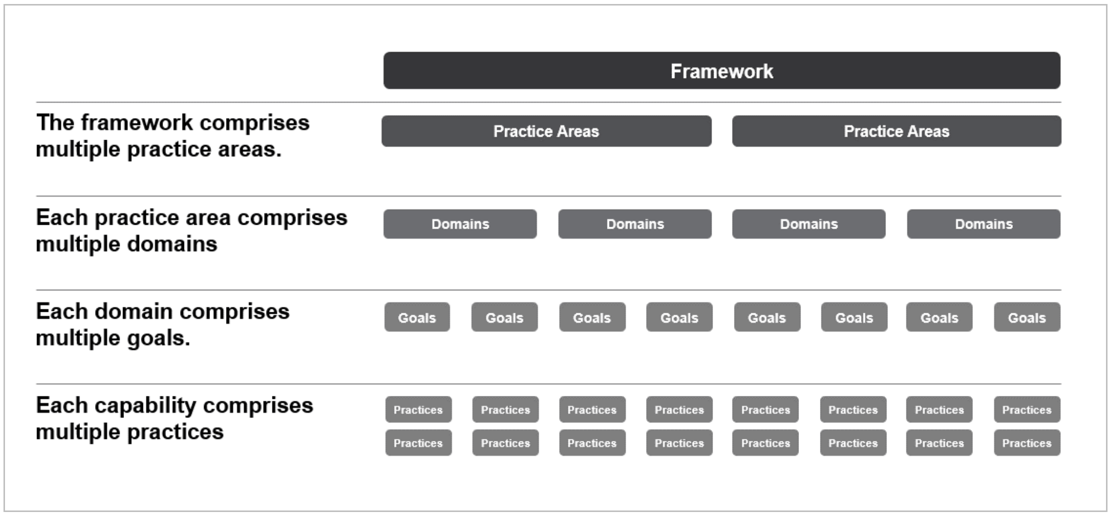
Framework
The framework comprises multiple practice areas.
Practice Areas
Practice Areas
Each practice area comprises multiple domains
Domains
Domains
Domains
Domains
Each domain comprises multiple goals.
Goals
Goals
Goals
Goals
Goals
Goals
Goals
Goals
Each capability comprises multiple practices
Practices

Figure 3: ASF Organization and Structure

The ASF is designed to foster collaboration across the range of stakeholders responsible for acquiring, developing, and deploying software-reliant systems. As a result, some practices across ASF goals, domains, and practices areas are interrelated and intended to support each other. For example, the ASF documents risk management practices for program management, engineering, and supplier management. We included links among the various risk practices to emphasize the importance of implementing integrated risk management processes (one of the three ASF challenges). Linking practices in this way highlights the information sharing and communication that should routinely occur across all program teams and suppliers.

[2] Assessments are a key aspect of security and resilience management. ASF practices are phrased as questions to facilitate the use of ASF content to assess a program's security and resilience practices. The framework and questions are included in Appendix A.

3.3 ASF Practice Area and Domain Summaries

In this section, we provide a short summary of each ASF practice area and highlight its associated domains. In the ASF, practice areas and domains establish the foundation for the ASF organizing structure. ASF practices are grouped into the following practice areas:

- Program Management
- Engineering Lifecycle
- Supplier Dependency Management
- Support
- Independent Assessment and Compliance
- Process Management

We have completed an initial draft of the practices for the first four practice areas listed above. We are starting to document practices for the remaining two practice areas: Independent Assessment and Compliance and Process Management. We include our initial draft of the goals and practices for the four completed practice areas in Appendix A.

3.3.1 Program Management

A program is a group of related projects and functions that are managed in a coordinated manner to achieve a common mission. From a traditional perspective, program management is focused on controlling cost, schedule, and performance. In the ASF, the Program Management practice area defines a set of practices for ensuring that security/resilience are addressed from the earliest stages of an acquisition and throughout the systems lifecycle. Including security/resilience considerations during a program's early planning and management activities provides a foundation for coordinated and integrated management of security/resilience across all program teams. The Program Management practice area also identifies security/resilience practices for requirements and risk management that are coordinated across the program and lifecycle. The Program Management practice area includes the following domains:

- *Domain 1, Program Planning and Management* integrates security/resilience into a program's planning and management activities.
- *Domain 2, Requirements and Risk* manages security/resilience requirements and risks at the program level.

See Appendix A for a list of goals and questions for each domain.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

3.3.2 Engineering Lifecycle

The term *engineering lifecycle* describes the range of management and technical activities needed to build and operate a system, from initial concept though development, production, deployment, and support. In the ASF, the Engineering Lifecycle practice area defines a set of practices for integrating security/resilience into a program's systems engineering and software engineering activities. In addition to addressing the technical aspects of security/resilience engineering, Engineering Lifecycle also ensures that the program's engineering activities are planned and managed, including those performed by third-party contractors. Finally, Engineering Lifecycle practices ensure that engineering processes, software, and tools (i.e., the engineering infrastructure) are secure and resilient, reducing the risk of attackers being able to disrupt program and system information and assets. The Engineering Lifecycle practice area includes the following domains:

- *Domain 1, Engineering Infrastructure* builds security/resilience into the engineering infrastructure and manage security/resilience risks to the engineering infrastructure over time.
- *Domain 2, Engineering Management* manages security/resilience requirements and risks across the engineering lifecycle.
- *Domain 3, Engineering Activities* integrates security/resilience into the program's engineering practices and processes.

See Appendix A for a list of goals and questions for each domain.

3.3.3 Supplier Dependency Management

Employing third-party/supplier support for systems development and operation has become a standard practice across the acquisition community. A broad network of contracted and non-contracted suppliers enables a program access to specialized skills, components, and infrastructure in a cost-effective manner. At the same time, these supplier relationships create dependency risks that must be managed in the context of the program's overall risk management strategy. Suppliers of products and services that are governed by contractual agreements require careful management and monitoring. Some suppliers, such as infrastructure providers and government service providers, do not typically rely on contracts to codify relationships, leading to dependency risks that are frequently overlooked. While non-contracted suppliers are often less of a concern, programs must manage security/resilience risks resulting from these dependencies as well. In the ASF, the Supplier Dependency Management practice area provides leading practices for managing dependencies that should be considered when building secure/resilient systems. The Supplier Dependency Management practice area includes the following domains:

- *Domain 1, Relationship Formation* includes security/resilience requirements and supplier risks in formal agreements with suppliers.
- *Domain 2, Relationship Management* manages the performance of suppliers and dependencies and ensures that security/resilience risks inherited from third-party relationships are managed.
- *Domain 3, Supplier Protection and Sustainment* includes third parties in the program's protection and sustainment activities.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

See Appendix A for a list of goals and questions for each domain.

3.3.4 Support

As it works toward its acquisition and development mission, a program requires support from a variety of organizational departments, groups, and teams. Organizational support activities provide a broad range of services, including security management, facility management, access management, measurement and analytics, and training. The Support practice area outlines leading practices that facilitate integrated support for acquiring, developing, and managing secure/resilient systems across their lifecycle. The Support practice area includes the following domains:

- *Domain 1, Program Support* ensures that security/resilience training, resources, and assistance are available to the program or system as needed.
- *Domain 2, Security Support* provides oversight and management of the program's security-related activities.

See Appendix A for a list of goals and questions for each of the four domains we discuss in this report.

3.3.5 Independent Assessment and Compliance

An independent assessment is an activity where individuals who are not directly connected with a program or system evaluate some or all aspects of that environment and report the results to designated stakeholders. Compliance is the act of conforming to the requirements outlined in the set of laws, regulations, policies, and standards that a program or system must meet. In the ASF, the Independent Assessment and Compliance practice area defines activities for reviewing a program or system to determine if it

- meets security/resilience requirements, including customer, product, and product component requirements
- fulfills its intended use when placed in its target environment

This practice area of the ASF is broad and addresses several lifecycle activities, including operational test and evaluation (OT&E) and authorization to operate (ATO). It also includes reviews of specialty areas, such as safety and nuclear surety.

The domains, goals, and questions for this practice area are under development and are not included in this report.

3.3.6 Process Management

Process management comprises practices that facilitate predictable and efficient delivery of program activities, putting the program in a position to achieve its security and resilience objectives. Process management practices help clarify and align an organization's strategies, policies, procedures, standards, and approach. A key premise of process management is that organizational outcomes are highly influenced by the quality of its processes. Higher degrees of process management translate to more stable environments that produce predictable results over time and help

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

enable mission success at lower risk. In addition, process management is based on the principle that change is continuous. Managing change in a program or system environment requires continual management and improvement of processes, helping to ensure that those processes continue to meet their objectives. A key challenge to every acquisition program is implementing an appropriate level of process management that reflects its environment, mission, and objectives. The ASF leverages process management to help ensure that the "right amount of cyber" is implemented across the program and its suppliers. In the ASF, the Process Management practice area defines activities for managing and improving the processes used to acquire, develop, and operate software-reliant systems.

The domains, goals, and questions for the Process Management practice area are under development and are not included in this report.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

4 Conclusion and Next Steps

Organizations face heightened and rapidly evolving challenges as they manage the risks affecting their software-intensive architectures. These challenges emanate from the demands of today's global marketplace, the dynamic nature of the threat environment, the pace of technological change, and the complexities brought on by the array of participants that must collaborate to develop and operate a system. Virtually all products and services an organization acquires are supported by or integrate with information technology that includes third-party components and services. Practices critical to monitoring and managing supplier and cyber risks are scattered, resulting in inconsistencies and coordination gaps.

The ASF contains leading practices designed to support programs building/acquiring secure, resilient software-reliant systems that are designed to manage risks across their lifecycle. Many security and resilience solutions focus on just a few aspects of engineering, such as security requirements specification, secure coding practices, or supply chain risk management. In contrast, the ASF leverages a proven set of integrated program management, engineering, and supplier management practices and processes that span the systems lifecycle.

An essential next step for the ASF development team is to communicate the value of the ASF and provide use cases to address challenges faced by virtually all organizations. Beyond that, we plan to continue to develop the ASF and refine it as we receive information from user feedback and implementations. Fortunately, awareness that all sectors must find better ways to manage the development and operation of resilient systems is emerging as the paramount technology issue. Organizations that help set the course for public and private discourse on cybersecurity and resilience, such as NIST, ISO, the U.S. Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and the SEI, have recognized the importance of acting and are actively exploring a path forward.

Our additional plans include using a variety of venues to communicate the value proposition of the ASF to leading organizations. We offer open access to ASF methods and materials as well as collaboration opportunities with the ASF development team. Some of the programs we believe can benefit the most from the ASF include organizations tasked with the following:

- providing an effective national defense
- managing risk to critical infrastructure
- ensuring reliable power and water
- providing critical government services
- supporting the monetary systems that are essential to promoting economic stability and growth

Lacking more resilient systems, organizations face increasing risk from man-made and natural threats.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Building the ASF is clearly a challenge, but the larger concern is making sure that the approach is usable by those who need it. To help users experience value quickly, we have been building methods for deploying the ASF in organizations that support software-intensive systems. These deployment methods include exploring the use of the ASF as a baseline roadmap of practices for engineering and supplier management to improve current program considerations of cybersecurity and supply chain risk. We do this by comparing program and vendor deliverables, such as statements of work, software assurance and cybersecurity checklists, and control plans, to the ASF. By mapping these program artifacts to ASF practices areas and goals, we can identify the practice areas that are already well addressed and gaps in practice areas that should be addressed. We also plan to make the ASF available to suppliers to help them strengthen their cyber risk management programs and meet the requirements of the organizations they support.

The ASF defines a comprehensive framework for building and operating secure and resilient software-reliant systems. Many programs will not be prepared to adopt the entire ASF at one time. However, these programs can still benefit by focusing on a single practice area, domain, or goal. To accommodate this class of adopter, we plan to develop and disseminate guidance for ASF practices. Guidance can include information about how to implement a practice, the competencies required to implement it, and the methods and tools that support it. For example, an engineering team that is interested in improving its software bill of materials (SBOMs) could review ASF guidance for third-party components to learn about SBOMs, including how to implement a solution in its program.

Technology and systems have become so essential that virtually every government and private organization has realized that resilience is a business imperative rather than a by-product of compliance. Cybersecurity vigilance is a shared global challenge, and resilience is an emergent property requiring ongoing collaborative effort by all of those involved with supporting a system over its lifecycle. The ASF is designed to provide a roadmap to facilitate that collaboration.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Appendix A: ASF Domains, Goals, and Questions

This appendix presents the domains, goals, and questions (i.e., practices) for the following four of the six ASF practice areas:

- Program Management
- Engineering Lifecycle
- Supplier Dependency Management
- Support

Program Management

Domain	Goal Name
Domain 1—Program Planning and Management	Program Definition
	Program Planning
	Program Monitoring and Management
	Communication and Coordination
Domain 2—Requirements and Risk	Program Requirements
	Program Risk Management

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Domain 1—Program Planning and Management

Program Definition

Goal 1—Security/resilience is addressed in conjunction with program definition and updated periodically.

The purpose of this goal is to ensure that security/resilience is considered during program definition activities.

1. Has the program defined its mission and objectives?
2. Are relevant security/resilience policies, standards, and guidelines identified, communicated, and understood?
3. Have security/resilience policies, standards, and guidelines been tailored to meet the program’s mission and objectives, including as circumstances change?
4. Are risk strategies that support the program’s mission and objectives developed and maintained?
5. Is risk integrated across all program teams in coordination with the governance and management structure?
6. Are security/resilience processes established and maintained for the program?
7. Is a lifecycle approach for managing security/resilience established and maintained by the program?
8. Are standard terms and definitions for security/resilience established and maintained for the program?

Program Planning

Goal 2—Security/resilience activities are integrated into the program plan.

The purpose of this goal is to ensure that security/resilience is included in the program plan.

1. Are security/resilience objectives for the program defined and documented?
2. Is there an established and communicated program plan that includes security/resilience activities, schedule, and budget?
3. Are security/resilience roles and responsibilities defined and assigned?
4. Are adequate resources (e.g., people, tools, facilities) to implement planned security/resilience tasks provided?
5. Is a program compliance initiative for security/resilience defined and implemented?
6. Are stakeholders knowledgeable about their security/resilience roles?
7. Are the criteria that define risks established for security/resilience capabilities and controls in the deployed system?

Program Monitoring and Management

Goal 3—Security/resilience activities are monitored and managed.

The purpose of this goal is to monitor and manage security/resilience activities across all program teams.

1. Are security/resilience tasks allocated and managed across all program teams?
2. Is the progress of the program’s security/resilience tasks monitored and updated as needed?
3. Is the security/resilience budget tracked and updated?
4. Is program compliance with security/resilience policies, laws, and regulations monitored and managed?
5. Are security/resilience reviews of program tasks performed?
6. Are the results of security/resilience reviews prioritized and addressed?
7. Is program decision making supported by security/resilience measurement and metrics?
8. Are stakeholders’ inputs for security/resilience included when making program management decisions?
9. Is the delivery of security/resilience capabilities into the user environment managed and facilitated?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Communication and Coordination

Goal 4—Security/resilience communication and coordination mechanisms and resources are defined and implemented.

The purpose of this goal is to provide mechanisms and resources for communicating and coordinating security/reliance across all program teams.

1. Is a security/resilience communication plan established and maintained?
2. Is the responsibility for security/resilience communication established and maintained?
3. Is security/resilience communication reviewed for effectiveness?
4. Are security/resilience governance and status reports distributed regularly to key stakeholders?
5. Are security/resilience activities, resources, and constraints communicated to all program teams and other appropriate stakeholders?
6. Is security/resilience communication between the customer and user representatives and the engineering teams facilitated?
7. Is security/resilience communication coordinated across all program teams and other appropriate stakeholders?
8. Are security/resilience activities coordinated and managed with all program teams and other appropriate stakeholders?
9. Are security/resilience risks coordinated and managed with related programs and systems?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Domain 2—Requirements and Risk

Program Requirements

Goal 1—Program security/resilience requirements are identified and managed.

The purpose of this goal is to ensure that security/resilience is part of program requirements management.

1. Are program security/resilience requirements elicited, categorized, and prioritized?
2. Are inspections of program security/resilience requirements performed to ensure their completeness and sufficiency?
3. Are the ownership and status of program security/resilience requirements tracked across the lifecycle?
4. Are program security/resilience requirements structured to ensure that traceability is maintained?
5. Are quality criteria for program security/resilience requirements established?
6. Are reviews conducted periodically to determine if program security/resilience requirements meet the established quality criteria?
7. Are triggers in place that require a review of program security/resilience requirements?
8. Are program security/resilience requirements updated periodically based on reviews?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Program Risk Management

Goal 2—Program security/resilience risks are identified and managed.

The purpose of this goal is to coordinate and manage security/resilience risks across all program teams.

1. Is a plan for managing program security/resilience risks established and agreed to by stakeholders?
2. Are program security/resilience risks (e.g., program risks related to security/resilience resources and funding, risks escalated from other groups) identified and tracked?
3. Are program security/resilience risks analyzed, prioritized, and addressed based on the program’s mission and objectives?
4. Are criteria to guide security/resilience risk escalation established and communicated across all program teams?
5. Are identified security/resilience risks escalated and dispositioned appropriately?
6. Are program- or system-wide security/resilience risk analyses informed by threat intelligence and situational awareness?
7. Are security/resilience risk analytics included in periodic updates to key stakeholders about risk management activities?
8. Are security/resilience risks for the program’s information technology systems and networks identified, managed, and tracked?
9. Are plans for dispositioning high-priority program security/resilience risks developed?
10. Are plans for dispositioning high-priority program security/resilience risks documented and tracked?
11. Are program security/resilience risks communicated to stakeholders?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Engineering Lifecycle

Domain	**Goal Name**
Domain 1—Engineering Infrastructure	Infrastructure Development
	Infrastructure Operation
Domain 2—Engineering Management	Technical Activity Management
	Product Risk Management
Domain 3—Engineering Activities	Requirements
	Architecture
	Third-Party Components
	Implementation
	Test and Evaluation
	Transition Artifacts
	Deployment
	Secure Product Operation

Domain 1—Engineering Infrastructure

Infrastructure Development

Goal 1—Security/resilience is built into the engineering infrastructure.

The purpose of this goal is to identify and manage security/resilience risks when specifying and developing the engineering infrastructure.

1. Has a lifecycle model (e.g., waterfall, Agile, DevSecOps) that includes security/resilience engineering been selected for the program?
2. Is a tradeoff analysis of performance and quality attributes for the engineering infrastructure, including security/resilience, performed?
3. Are security/resilience requirements established for the engineering infrastructure?
4. Are security/resilience processes, software, and tools for the engineering infrastructure selected and implemented?
5. Is a baseline security/resilience configuration for the engineering infrastructure defined and implemented?
6. Is intelligence data for security/resilience (e.g., attack data, vulnerabilities, design weaknesses, abuse/misuse cases, and threats) collected and maintained?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Infrastructure Operation

Goal 2—Security/resilience risks in the engineering infrastructure are identified and mitigated.

The purpose of this goal is to manage security/resilience risks in the engineering infrastructure.

1. Are security/resilience risks in the engineering infrastructure’s systems and networks assessed and managed?
2. Is user access to the engineering infrastructure’s systems, software, and tools managed?
3. Are the engineering infrastructure’s systems and networks monitored for unusual activity?
4. Are patches and updates to the engineering infrastructure’s systems and networks applied when needed?
5. Are the engineering infrastructure’s data, applications, and tools backed up periodically?
6. Are incidents affecting the engineering infrastructure identified and managed?
7. Is a service continuity plan defined for the engineering infrastructure?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Domain 2—Engineering Management

Technical Activity Management

Goal 1—Engineering activities are planned and managed.

The purpose of this goal is to oversee the execution of engineering activities, including those performed by third-party contractors.

1. Is a plan for conducting the engineering activity developed and implemented?
2. Is progress against the plan tracked and reported?
3. Are criteria established for reviewing and accepting acquisition and engineering work products?
4. Are acquisition and engineering work products reviewed and accepted?
5. Are issues and risks that can affect engineering activities identified and resolved?
6. Are issues and risks that can affect engineering activities escalated to program management and other stakeholders as appropriate?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Product Risk Management

Goal 2—Security/resilience risks that can affect the system and its associated work products are identified, managed, and tracked across all lifecycle phases.

The purpose of this goal is to analyze security/resilience risks in high-priority system components, including analysis of threats, weaknesses, vulnerabilities, access points, and attack paths.

1. Are the system's mission, operating environment, and compliance requirements analyzed and understood by the engineering technical staff?
2. Are confidentiality, integrity, and availability requirements established for the data that the system will store, process, and transmit?
3. Is a first-pass (e.g., high-level) risk assessment of the system and its technology conducted to identify critical system components?
4. Are security/resilience risks that can affect high-priority system components identified?
5. Are security/resilience risks that can affect high-priority system components analyzed and prioritized?
6. Are plans for dispositioning high-priority security/resilience risks developed?
7. Are security/resilience risk assessment results communicated to stakeholders?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Domain 3—Engineering Activities

Requirements

Goal 1—Security/resilience requirements for systems and system components are specified, analyzed, and managed.

The purpose of this goal is to specify the security/resilience needs or capabilities that the system should provide.

1. Are security/resilience requirements elicited, categorized, and prioritized?
2. Are inspections of security/resilience requirements performed to ensure completeness and sufficiency?
3. Are security/resilience requirements structured to ensure that traceability is maintained?
4. Are quality criteria for security/resilience requirements established?
5. Are reviews conducted periodically to determine if security/resilience requirements meet established quality criteria?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Architecture

Goal 2—Security/resilience risks resulting from the architecture and design are identified and mitigated.

The purpose of this goal is to identify and mitigate security/resilience risks resulting from the system's architecture and detailed design.

1. Is a security/resilience risk analysis of the architecture and detailed design performed?
2. Are identified security/resilience risks from the architecture and detailed design managed and tracked?
3. Is an architecture tradeoff analysis of quality attributes, including security/resilience, performed?
4. Are security/resilience risks resulting from architecture tradeoffs communicated to stakeholders?
5. Is the architecture's attack surface minimized based on the results of an attack-path analysis?
6. Is a cross check of the architecture and detailed design performed to resolve any issues or inconsistencies in security/resilience features?
7. Are security/resilience requirements updated periodically to reflect security/resilience changes to the architecture and detailed design?
8. Are reviews conducted with stakeholders to ensure that security/resilience risks resulting from the architecture and detailed design are mitigated sufficiently?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Third-Party Components

Goal 3—Security/resilience risks that can affect third-party components (TPCs) are identified and mitigated.

The purpose of this goal is to develop a bill of materials (BOM) for a product and ensure that operational security/resilience risks in the third-party software, firmware, and hardware are managed over time.

1. Are engineering relationships with third parties based on standards, guidelines, and policies?
2. Is a scheme that uniquely identifies each third-party component (TPC) implemented?
3. Is a repository to track TPC use in products implemented and maintained?
4. Are TPCs that are used in products identified and documented to create a bill of materials (BOM)?
5. Are suppliers evaluated and selected based on their use of secure/resilient development practices?
6. Is each TPC's operational risk assessed?
7. Are TPCs monitored for vulnerabilities and available updates?
8. Are TPCs prioritized for patch application based on operational risk?

Implementation

Goal 4—Vulnerabilities in software code are identified, managed, and tracked.

The purpose of this goal is to identify and address vulnerabilities and security/resilience issues in the code base.

1.	Is an appropriate suite of security/resilience tools integrated into the software development environment?
2.	Are secure coding standards applied?
3.	Are code reviews (e.g., peer reviews) performed to identify weaknesses and vulnerabilities?
4.	Is source code in critical components analyzed using white-box testing (e.g., static code analysis) during coding and unit testing to identify weaknesses and vulnerabilities?
5.	Is software in critical components analyzed using black-box testing (e.g., dynamic code analysis, vulnerability scanning) during integration testing to identify weaknesses and vulnerabilities?
6.	Are coding weaknesses and vulnerabilities remediated and tracked to resolution?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Test and Evaluation

Goal 5—Security/resilience risks that can affect the integrated system are identified and remediated during test and evaluation.

The purpose of this goal is to verify the system's security/resilience requirements and assess the security/resilience of a system under realistic operational conditions.

1. Is there a requirement to obtain an authorization to assess security/resilience during test and evaluation?
2. Are test plans and artifacts for security/resilience developed and updated?
3. Are security/resilience test-and-evaluation activities performed in an operationally relevant environment?
4. Are tests of the system and software security/resilience requirements performed?
5. Are vulnerability evaluations of the system performed?
6. Are adversarial assessments (e.g., red team exercises) of the system performed?
7. Are security/resilience risks identified by analyzing weaknesses and vulnerabilities discovered during test and evaluation?
8. Are security/resilience risks identified during test and evaluation remediated or mitigated?
9. Are security/resilience risks identified during test and evaluation communicated to stakeholders?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Transition Artifacts

Goal 6—Documentation and tools that support the secure operation and sustainment of the system are developed and distributed.

The purpose of this goal is to provide tools and information that facilitate security/resilience management after a system is deployed.

1. Is security/resilience information for system administrators and users, such as configuration practices and user practices, compiled and documented?
2. Are security/resilience management tools for the system developed, procured, and supplied to the operational support organization?
3. Are security/resilience documentation and support tools reviewed before they are released to the operational support organization and other system stakeholders?

Deployment

Goal 7—System components are protected during transport and installation.

The purpose of this goal is to ensure that security/resilience risks that can affect software, firmware, and hardware are managed during their transport and installation.

1. Is the security group’s sign-off required before a system can be deployed into its operational environment?
2. Is responsibility for managing security/resilience risks after deployment transferred to the operational support organization?
3. Are software, firmware, and hardware components protected from tampering and modification during their transport and installation?
4. Is the integrity of all deployed software, firmware, and hardware verified?
5. Are confidentiality and integrity risks for sensitive data (e.g., passwords, tokens) mitigated adequately for software that operates in operational environments?

Secure Product Operation

Goal 8—Security/resilience risks and issues are identified and resolved as the system is used and supported in the operational environment.

The purpose of this goal is to analyze operational risks and issues and initiate changes to the system support package for the operational system.

1. Are periodic security/resilience risk assessments of the operational system performed?
2. Are periodic penetration testing and vulnerability scanning of the operational system performed to identify vulnerabilities?
3. Is the behavior of the operational system monitored to identify signs of attack?
4. Are security/resilience practices monitored during operations and sustainment?
5. Are confidentiality, integrity, and availability requirements for system data reassessed periodically during operations and sustainment?
6. Are vulnerabilities, threats, and risks identified and tracked to closure?
7. Are protection strategies (e.g., program protection plan, security/resilience controls) for the operational system updated periodically or when the threat profile changes?
8. Is data collected, analyzed, and communicated to provide adequate situational awareness of the operational system’s threat environment?
9. Are changes to the operational system’s risk posture reported to the authorizing official in accordance with the monitoring strategy?
10. Are patches applied to the operational system when appropriate?
11. Are disruptions that affect the operational system managed?
12. Are suggested system changes or improvements related to security/resilience communicated to the engineering team?
13. Is a decommissioning strategy defined for addressing security/resilience concerns when the operational system is removed from service?
14. Is automation implemented where feasible to enable more effective security/resilience risk management during operations and sustainment?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Supplier Dependency Management

Domain	Goal Name
Domain 1—Relationship Formation	Supplier Relationship Planning
	Supplier Requirements
	Supplier Evaluation
	Supplier Risk Management
Domain 2—Relationship Management	Supplier Prioritization
	Supplier Performance Management
	Supplier Risk Management
	Supplier Change and Capacity Management
	Supplier Access
	Infrastructure and Governmental Dependencies
	Supplier Transitions
Domain 3—Supplier Protection and Sustainment	Supplier Disruption Planning
	Supplier Planning and Controls
	Supplier Situational Awareness

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Domain 1—Relationship Formation

Supplier Relationship Planning

Goal 1—Establishing supplier relationships is planned.

The purpose of this goal is to assess whether entering into relationships with suppliers is planned.

1. Is entering into formal agreements with suppliers planned?
2. Are baseline (i.e., boilerplate) requirements that apply to any supplier that supports the program or system identified and documented?
3. Are security/resilience requirements identified and documented for any supplier (e.g., contracted suppliers, infrastructure providers, and governmental services providers) that supports the program or system?
4. Are security/resilience requirements considered before agreeing to relationships with suppliers?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Supplier Requirements

Goal 2—Security/resilience requirements are included in formal agreements with suppliers.

The purpose of this goal is to assess whether supplier agreements include security/resilience requirements.

1. Are security/resilience requirements included in formal agreements?
2. Are requirements for reporting incidents to the program office and/or system manager included in formal agreements?
3. In formal agreements, are suppliers required to manage vulnerabilities that might affect the program or system?
4. In formal agreements, are suppliers required to maintain disruption management plans?
5. In formal agreements, are suppliers required to participate in disruption management planning and exercises?
6. In formal agreements, are suppliers required to manage their own suppliers?

Supplier Evaluation

Goal 3—Suppliers are evaluated before entering into formal relationships with them.

The purpose of this goal is to assess whether suppliers are evaluated to determine if they can meet the security/resilience requirements for the program or system before entering into relationships.

1. Are criteria used to evaluate the supplier’s ability to meet security/resilience requirements?
2. Are security/resilience requirements included in written communications with prospective suppliers, for example in requests for proposals?
3. Is the supplier’s ability to meet security/resilience requirements of the program or system considered before entering into a formal relationship with that supplier?
4. Are suppliers that require documented verification of their ability to meet the system or program security/resilience requirements identified?
5. Are the supplier’s own supplier risks reviewed and evaluated before entering into agreements with that supplier?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Supplier Risk Management

Goal 4—Supplier risk is managed.

The purpose of this goal is to assess whether risk management is included in supplier risk considerations.

1. Is there a plan for managing the operational risk been established and agreed to by Stakeholders?
2. Are the risks of relying on suppliers to support the program or system identified and managed (accepted, avoided, transferred, mitigated, etc.)?
3. Are risk criteria established and used to avoid or reject suppliers?
4. Are the risks of a supplier being a single point of failure identified?

Domain 2—Relationship Management

Supplier Prioritization

Goal 1—Suppliers are identified and prioritized.

The purpose of this goal is to assess whether suppliers that the program or system depends on are identified and prioritized.

1. Are dependencies on suppliers that are critical to the program or system identified?
2. Are suppliers prioritized?
3. Is there a tracking approach that provides a current list of suppliers?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Supplier Performance Management

Goal 2—Supplier performance is governed and managed.

The purpose of this goal is to assess whether performance is considered when evaluating suppliers that support the security/resilience of the program or system.

1. Is the performance of suppliers monitored against the security/resilience requirements of the program or system?
2. Is the responsibility for monitoring and managing the supplier established and maintained?
3. Are supplier performance issues documented and reported to the appropriate stakeholders?
4. Are corrective actions taken to address issues with supplier performance?
5. Are corrective actions evaluated to ensure issues are remedied?

Supplier Risk Management

Goal 3—Supplier risk management is continuous.

The purpose of this goal is to assess whether the risks of relying on suppliers to support the program or system are continuously managed.

1. Are security/resilience requirements for suppliers periodically reviewed and updated?
2. Are risks due to suppliers periodically reviewed?
3. Are periodic discussions held with suppliers to review risks?
4. Are periodic reviews with suppliers conducted to verify that vulnerabilities relevant to the program or system are continuously managed?
5. Is threat monitoring in place for all aspects of the program or system that are controlled by or connected to supplier systems?
6. Is automated alert notification used for supplier threat monitoring?
7. Are threats that pose material risk to the program or system identified?
8. Does risk monitoring include security/resilience requirements not codified in supplier agreements?
9. Are supplier performance issues and concerns included in risk monitoring?

Supplier Change and Capacity Management

Goal 4—Change and capacity management include suppliers.

The purpose of this goal is to assess whether change and capacity management are coordinated with suppliers that support the program or system.

1. Is change management used for managing modifications to the assets of the program or system
2. Are changes to assets (whether located internally or at a supplier’s location) coordinated among the suppliers and the stakeholders of the program or system?
3. Is a review of disruption management plans triggered when there are changes at an external entity?
4. Are contract renegotiations, updates, addenda, and similar changes tracked to identify and manage impacts to the program or system?
5. Is there monitoring of organizational changes at suppliers - for example buy- outs, financial problems, political or civil problems - that may affect the program or system?
6. Is the capacity of services and assets cooperatively managed with suppliers?

Supplier Access

Goal 5—Supplier access to program or system assets is managed.

The purpose of this goal is to assess whether the risks associated with supplier access to assets is managed. (These questions involve access granted to any supplier, not only those that support the program or system.)

1. Is access to assets that support the program or system granted to suppliers (locally or remotely) based on the assets’ protection requirements?
2. Are changes to supplier access privileges managed when there are supplier personnel changes such as terminations, promotions, or job changes?
3. Is access that is granted to supplier personnel or systems periodically reviewed to identify inappropriate access privileges?
4. Are all identified issues with supplier access privileges addressed?
5. Are inappropriate or unusual access attempts by supplier personnel or systems routinely identified?
6. Are there appropriate controls that incorporate network segregation (where appropriate) to protect network integrity when suppliers are involved?

Infrastructure and Governmental Dependencies

Goal 6—Infrastructure and governmental dependencies are managed.

The purpose of this goal is to assess whether the risks of depending on infrastructure providers and/or government service providers are identified and managed.

1. Are security/resilience requirements for infrastructure and government providers that support the program or system periodically reviewed and updated?
2. Is someone in the organization responsible for monitoring the performance of infrastructure providers that support the program or system?
3. Is someone in the organization responsible for managing relationships with government service providers that support the program or system?
4. Are issues involving infrastructure providers and government service providers communicated to stakeholders to enable them to manage the dependency?
5. Are issues involving infrastructure providers and government service providers included in risk monitoring?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Supplier Transitions

Goal 7—Supplier transitions are managed.

The purpose of this goal is to assess whether managing the transition of supplier relationships is based on business considerations (e.g., insolvency, nonperformance, new technology).

1.	Are criteria or conditions that would cause the termination of formal agreements with suppliers identified?
2.	Are there plans or actions for sustaining the program or system if any formal agreement with a supplier is terminated by either the acquirer or supplier?
3.	Are lessons learned from supplier transitions used to refine the supplier management approach for the program or system?

Domain 3—Supplier Protection and Sustainment

Supplier Disruption Planning

Goal 1—Suppliers are included in disruption planning.

The purpose of this goal is to assess whether suppliers are included in incident management and service continuity for the program or system.

1. Is there an incident management plan established for protecting the program or system?
2. Are incident declaration criteria that support the program or system established and communicated to relevant suppliers?
3. Are past events and incidents reviewed to determine whether they pose a material risk to the program or system?
4. Is the dependence on suppliers considered when forming program or system disruption plans?
5. Do relevant suppliers participate in disruption planning?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Supplier Planning and Controls

Goal 2—Planning and controls are maintained.

The purpose of this goal is to assess whether program or system controls and plans related to suppliers are regularly tested and updated.

1. Are disruption management (e.g., incident, service continuity) plans tested cooperatively with relevant suppliers?
2. Are controls at suppliers that support the program or system periodically validated or tested to ensure they meet control objectives?
3. Are mechanisms (e.g., load balancing, encryption, integrity checking) used to meet security/resilience requirements at suppliers under normal and adverse situations?
4. Are triggering events and changes (criteria) that require the testing of controls at suppliers that support the program or system defined and documented?
5. When triggering criteria are met that require the testing of controls, is testing conducted?
6. Are communications to internal and external stakeholders (e.g., executive and management teams) included in program or system recovery activities?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Supplier Situational Awareness

Goal 3—Suppliers are included in situational awareness reviews and analysis.

The purpose of this goal is to assess whether situational awareness activities for the program or system include suppliers. (Satisfying this goal means that information sources about threats to key suppliers are monitored for the sake of the program or system.)

1. Is someone in the organization responsible for monitoring sources of threat information?
2. Is threat monitoring—including how threats, events, and incidents are received and responded to—used to protect the program or system?
3. Are suppliers identified that should be included in threat monitoring for the program or system?
4. Is relevant information about threats to the program or system exchanged with suppliers?
5. Are industry consortia (i.e., InfraGard, Coordinating Councils, Council of Supply Chain Management) resources utilized when managing threats to the program or system and key suppliers?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Support

Domain	Goal Name
Domain 1—Program Support	Security/Resilience Training
	Measurement and Analysis
	Configuration and Change Management
	Resource Coordination and Management
Domain 2—Security Support	Security Administration
	Asset Management
	Information and Records Management
	Access Management
	Facility Management
	Disruption Management

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Domain 1—Program Support

Security/Resilience Training

Goal 1—Security/resilience training is provided to personnel.

The purpose of this goal is to ensure that personnel have the security knowledge and skills required to perform their job functions adequately.

1. Are security/resilience training needs (both general security/resilience and role based) established and maintained?
2. Are plans for security/resilience training for personnel (including suppliers) established and maintained?
3. Is security/resilience training for personnel provided periodically?
4. Is role-based security/resilience training for technical personnel (including vendors, contractors, and outsourced workers) provided as required?
5. Are gaps in the role-based security/resilience skills of personnel identified and tracked?
6. Is the completion of security/resilience training activities (including the activities of suppliers) tracked?
7. Is the effectiveness of security/resilience training reviewed?
8. Is security/resilience training updated periodically based on effectiveness reviews?
9. Is data classification training provided to employees and contractors?

Measurement and Analysis

Goal 2—Security/resilience measurement data is collected, analyzed, and used to support decisions.

The purpose of this goal is to support monitoring and effective decision making based on security/resilience measurement.

1. Is there a plan for the measurement and analysis of security/resilience activities?
2. Is data about security/resilience measurement collected and communicated to relevant stakeholders according to the plan?
3. Are measurement and analysis gaps in the plan identified?
4. Are plan measurement and analysis gaps communicated to relevant stakeholders?
5. Is data about security/resilience measurement managed according to the plan?
6. Is data about security/resilience measurement analyzed and interpreted to support risk decisions?
7. Are security/resilience measurement objectives identified?
8. Are security/resilience measures that address measurement objectives identified?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Configuration and Change Management

Goal 3—Security/resilience configuration items (e.g., requirements specifications, architecture documentation, code, user documents, and support tools) are identified, managed, and tracked.

The purpose of this goal is to ensure the consistency of security/resilience configuration and change-management activities across all teams.

1. Is configuration management in place for all software and hardware components across the system’s lifecycle and suppliers?
2. Is change management in place for all software and hardware components across the system’s lifecycle and suppliers?
3. Are security/resilience configuration items identified?
4. Are baselines for security/resilience configuration items established, managed, and tracked?
5. Are change requests for security/resilience configuration items managed and tracked?
6. Are configuration audits performed throughout the system’s lifecycle to maintain the integrity of security/resilience configuration baselines?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Resource Coordination and Management

Goal 4—Security/resilience resources are established, coordinated, and managed.

The purpose of this goal is to ensure that adequate security/resilience resources are available to support all teams.

1. Is a repository established and maintained for security/resilience policies, standards, and guidelines?
2. Is a repository established and maintained for assets (e.g., people, technology, facilities, and information)?
3. Is data about security/resilience risk (e.g., attack data, vulnerabilities, design weaknesses, abuse/misuse cases, threats) collected and maintained?
4. Are security/resilience risk registers established and maintained by all teams?
5. Is guidance for classifying data established and managed?
6. Are security experts made available to supplement team skills as needed?
7. Are periodic reviews of resource adequacy conducted?

Domain 2—Security Support

Security Administration

Goal 1—Program security activities are coordinated, tracked, and managed.

The purpose of this goal is to ensure that security-related oversight and documentation activities are performed and managed.

1. Are security policies and procedures for technology (e.g., hardware, software, networks) and devices established and maintained?
2. Is an acceptable-use policy established and maintained?
3. Are disruptions, problems or event-management activities tracked and managed?
4. Are security testing results tracked and managed to ensure requirements are met?
5. Are audits and assessments performed periodically?
6. Are independent security audits of internal and external activities conducted?
7. Do all personnel meet the security requirements of their jobs?
8. Is compliance with security standards, laws, and regulations managed by the program?
9. Are security-related activities monitored and managed by the program’s legal and contracting subject matter experts (SMEs)?

Asset Management

Goal 2—Program assets are inventoried, managed, and tracked over their lifecycle.

The purpose of this goal is to identify high-value assets so that they can be managed and tracked throughout their lifecycle.

1. Are assets (i.e., people, information, technology, and facilities) inventoried?
2. Are assets managed and tracked throughout their lifecycle?
3. Are asset inventories reviewed and updated periodically?
4. Are asset owners and custodians identified for each asset?
5. Do guidelines exist for properly disposing of information assets?
6. Are the locations of assets documented in the asset database?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Information and Records Management

Goal 3—Information assets and records are managed according to their requirements.

The purpose of this goal is to ensure that information assets and records are managed according to their requirements.

1. Do policies and procedures exist for the proper security category labeling and handling of information assets (i.e., public, private, classified, secret etc.)?
2. Are personnel who handle information assets (including those from outside the organization, such as contractors) trained how to use information labeling categories?
3. Are security/resilience requirements tracked in the asset-management database?
4. Are where assets are located in accordance with requirements?
5. Are requirements used to determine which personnel have the authority to modify information assets?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Access Management

Goal 4—Access to program assets is managed according to their requirements.

The purpose of this goal is to ensure that access to assets is managed in a risk-informed manner throughout their lifecycle.

1. Is access (including identities and credentials) to assets granted based on their security and resilience requirements?
2. Are access permissions managed according to the principle of least privilege?
3. Are access permissions managed according to the principle of separation of duties?
4. Are access privileges reviewed to identify excessive or inappropriate privileges?
5. Are access privileges modified based on reviews?
6. Are identities (e.g., user accounts) validated before they are bound to credentials that are asserted in interactions?
7. Is remote access managed and monitored?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Facility Management

Goal 5—Security of the program’s physical workspaces and facilities is managed according to requirements.

The purpose of this goal is to facilitate effective management of facility-related risks and disruption impacts.

1. Are facilities prioritized according to their potential impact to identify those that should be the focus of protection and sustainment activities?
2. Is the accuracy of facility prioritization reviewed and validated?
3. Are protection and sustainment requirements considered when selecting facilities?
4. Are security policies and procedures for physical workspaces and facilities established and maintained?
5. Is access to restricted and protected areas by personnel managed?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Disruption Management

Goal 6—Events, incidents, and disruptions are managed according to the disruption management plan.

The purpose of this goal is to manage events and disruptions in a risk-aware manner that limits impact to the organization’s ability to achieve its mission.

1. Is there a plan for managing disruptions throughout the lifecycle?
2. Is the disruption-management plan reviewed and updated?
3. Are assets’ resources allocated to the roles and responsibilities outlined in the disruption management plan?
4. Are events, incidents, and disruptions detected and reported, including cybersecurity events related to personnel activity, network activity, the physical environment, and information?
5. Is information about disruptions communicated to internal and external stakeholders?
6. Are disruptions managed according to the plan?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Appendix B: Glossary

A common understanding of the meaning of words is essential to communication, measurement, and management. To that end, we have been developing a glossary for ASF terminology throughout the process of building framework. While this glossary is a work in process, we hope that the following definitions will provide the foundation for using the ASF.

The definitions in this glossary were derived from the following sources:

- NIST Computer Security Resource Center *Glossary* [NIST 2022]
- International Standard ISO/IEC/IEEE 24765:2017 *Systems and software engineering—Vocabulary* [ISO/IEC/IEEE 2017]
- *CERT Resilience Management Model: A Maturity Model (CERT-RMM) A Maturity Model for Managing Operational Resilience* [Caralli 2010]

Acquirer

An organization/program that depends on external entities (e.g., vendors, infrastructure providers, government, other business units) to fulfill its mission or business objectives (*Acquirer* refers to the assessed or subject organization.)

Acquirer Assets

Assets whose viability, productivity, and resilience are primarily the responsibility of the acquirer

Adversarial Assessment

An independent assessment that the measures the ability of an organization or system to carry out its mission adequately while withstanding cyber attacks

Architecture Tradeoff Analysis (or Architecture Tradeoff or Tradeoff Analysis)

See *Tradeoff Analysis*.

Assets

People, information, technology, and facilities that are used to provide the critical service being assessed (Several practices in the ASF refer to acquirer or external assets.)

Assurance

Grounds for justified confidence that a claim has been or will be achieved

Attack-Path Analysis

Analysis of the source or method used to commit a malicious action or interaction with the system or its environment that has the potential to result in a fault, an error (and thereby possibly in a failure), or an adverse consequence

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Automated Alert Notification

A process or piece of equipment that informs an individual or group of an event under specified conditions and functions without human intervention

Bill of Materials (BOM)

Documented formal hierarchical tabulation of the physical assemblies, subassemblies, and components needed to fabricate a product

Business Continuity

The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption

Capacity Management

The process of managing the demand for technology assets over a range of operational needs

Change Management (Change Control)

A continuous process used to control changes to information or technology assets, their related infrastructure, or any aspect of services, enabling approved changes to be implemented with minimum disruption (*Change management* is also known as *change control*.)

Clear-Box Testing

A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object (*Clear-box testing* is also known as *white box testing*.)

Code Review

Meeting where software code is presented to project personnel, managers, users, customers, and/or other interested parties for comment or approval

Confidentiality, Integrity, and Availability (CIA)

Often called the security triad and comprises three objectives

- Confidentiality—Only the authorized user/system/resource can view, access, change, or otherwise use information or data.
- Integrity—The system is able to ensure that information or data is accurate and correct.
- Availability—Systems, information, and services are accessible and usable when needed.

Control

A manual or automated method, policy, or procedure that an organization adopts to ensure the safeguarding of assets, the accuracy and reliability of management information and financial records, administrative efficiency, and adherence to standards

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Cooperative

Activities or processes that are jointly performed in a coordinated manner by a group of entities, individuals, or projects

Crisis

A critical state of affairs in which a decisive, probably undesirable outcome is impending

Critical Service

Activities an organization/program completes in performing a duty or creating a product that is essential to its mission

Cybersecurity

The ability to protect or defend the use of cyberspace from cyber attacks

Decommission

Withdraw from service or use

Dependency

A condition in which the functioning, production, or requirements of one or more entities, products, or services rely on the actions or state of another entity, product, or service

Disruption Management

Management activities that mitigate the impact of events that may negatively affect a critical service (Disruption management usually involves activities such as incident management, problem management, service/business continuity, crisis planning, or crisis response.)

Disruption Planning

Planning activities that manage and mitigate the impact of events that may negatively affect the critical service (Disruption planning usually involves activities such as incident management, problem management, service/business continuity, or crisis planning.)

Domain

In the context of the ASF, a logical grouping of practices that contribute to the cyber resilience and cybersecurity of an organization/program or system

Enterprise

An organization with a defined mission/goal and a defined boundary using information systems to execute that mission and with responsibility for managing its own risks and performance (An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management [e.g., budgets], human resources, security, information systems, information, and mission management.)

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

External Assets

Assets (i.e., people, information, technology, facilities) for which external entities are primarily responsible in terms of the assets' viability, productivity, and resilience

External Dependency

A condition where the production and requirements of one or more products or services provided by the acquirer depend on the actions of an external entity (This dependency usually happens because the external entity is a supplier of goods or services to the acquirer; the external entity has access to, ownership of, control of, responsibility for, or some other defined obligation relating to an asset that is important to the critical service.)

External Entity

An organization that is separate from the acquirer or business unit (While external entities are frequently separate legal entities, they may also be separate business units, affiliates, or divisions within a large enterprise.)

Formal Agreement

A written agreement that creates obligations between the acquirer and an external entity (Formal agreements can clarify terms, requirements, and responsibilities. Examples of formal agreements include contracts, service level agreements, or operational level agreements. Formal agreements are not required for an external dependency or relationship between an acquirer and external entity.)

Functional Testing

Testing conducted to evaluate the compliance of a system or component with specified functional requirements (*Functional testing* is also known as *black-box testing*.)

Governance

The process of establishing and enforcing strategic goals and objectives, organizational policies, and performance parameters

Government Service Providers

A state, local, tribal, or federal entity providing a product or service

Governmental Services

A service provided to people, organizations, or other entities in a political subdivision (e.g., nation, state, or locality) that is usually provided by a governmental department or agency (These services frequently involve security [e.g., fire, police]. Non-emergency examples include the U.S. Postal Service and transportation management and support agencies [e.g., federal and state agencies, regional port authorities].)

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Guidelines

Official recommendations or advice that specifies policies, standards, or procedures for how something should be accomplished

High-Value Service

See *Critical Service*.

Incident

An event or series of events that significantly affects (or has the potential to significantly affect) assets and services and requires the acquirer—and possibly external entities—to respond in some way to prevent or limit adverse impacts

Incident Declaration Criteria

Established requirements or characteristics that can be used to guide the determination of when an event or disruption should be declared to be an incident, typically requiring that a pre-established plan be invoked

Incident Management Plan

The documented predetermined set of instructions or procedures to detect, respond to, and limit consequences of a disruption or cyber attack against an organization

Information and Communications Technology (ICT)

Technology that encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information

Information and Communications Technology (ICT) Supply Chain

A linked set of resources and processes shared among acquirers, integrators, and suppliers that begins with the design of ICT products and services and extends through developing, sourcing, manufacturing, handling, and delivering ICT products and services to the acquirer

Infrastructure Providers

A type of organization that supplies goods or services to a region, economy, infrastructure sector, or political subdivision, and with which the acquirer normally has no commercially practical ability to negotiate the terms and conditions of agreements (Contracts with infrastructure providers are generally “take it or leave it.” Examples include natural gas, water, power, or transportation providers.)

Lifecycle Model

Framework containing the processes, activities, and tasks involved in the development, operation, and maintenance of a software product, spanning the life of the system from the definition of its requirements to the termination of its use

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Maturity Indicator Level (MIL)

A measure of the level of process institutionalization and the corresponding description of the attributes that indicate that level of mature capability (Higher levels of institutionalization translate to more stable processes that produce consistent results over time and that are retained during times of operational stress.)

Measurement and Metrics

(1) Act or process of assigning a number or category to an entity to describe an attribute of that entity; (2) assignment of numbers to objects in a systematic way to represent properties of the object; (3) assignment of a value (e.g., a number or category) from a scale to an attribute of an entity

Monitoring

Continual checking, supervising, critically observing, or determining the status to identify change from the performance level required or expected

Network Segregation

A process or approach that separates various critical and non-critical network elements (Typically, the goal of network segregation is to manage traffic flow between subnets based on established guidelines or policies.)

Operational Resilience

An organization's ability to adapt to risks that affect its core operational capabilities (Operational resilience is the emergent property of an organization that enables it to continue to survive and carry out its mission after disruptions that do not exceed its operational limit.)

Operational Risk

The potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence (Managing risk in the ASF focuses on operational risks involving the actions of people, technology failures, failed internal processes, and disruptive external events. Operational risk is distinct from, but related to, other enterprise risk areas, such as cost and schedule risk.)

Penetration Testing

A method of testing where testers target individual binary components or the application as a whole to determine whether intra or intercomponent vulnerabilities can be exploited to compromise the application, its data, or its environmental resource

Performance

The action or process of carrying out or accomplishing an action, practice, task, or function

Plan

A detailed, written formulation of a program of action to satisfy or perform a practice or goal

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Policy

A high-level, overall plan that embraces the general goals and acceptable procedures of an organization

Practice

An activity performed to support an ASF domain goal

Problem Management

The act of addressing or managing a difficulty, uncertainty, or otherwise realized and undesirable event, set of events, condition, or situation that requires investigation and corrective action

Process

(1) A series of actions or steps taken to achieve a particular ASF practice or goal (2) activities that can be recognized as implementations of practices (These activities can be mapped to one or more practices to allow the framework to be useful for process improvement.)

Program Management

The development, procurement, integration, modification, operation and maintenance, and/or final disposition of a group of activities, projects, systems, or group of systems

Quality Attributes or Criteria

Characteristics, criteria, or requirements directed at establishing a codified view of quality

Regulations

Requirements imposed by a governmental body (These requirements can establish product, process, or service characteristics, including applicable administrative provisions that have government-mandated compliance.)

Relationship

A connection, association, or some level of external dependency

Request for Proposal

A collection of formal documents that includes a description of the desired form of response from a potential supplier, the relevant statement of work for the supplier, and required provisions in the supplier agreement

Requirements Management

Activities that ensure requirements are identified, documented, maintained, communicated, and traced throughout the lifecycle of a system, product, or service

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Resilience

The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions (Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.)

Resilience Requirement

A constraint that the acquirer places on internal or external assets to ensure they remain viable and sustainable when used in production to support a service (Resilience requirements are often expressed in terms of confidentiality, integrity, or availability. These requirements help ensure the protection of high-value assets and their continuity when an incident or disruption occurs.)

Risk

See *Operational Risk*.

Risk Analysis

The process of examining identified risk factors for their probability of occurrence, potential loss, and potential risk-handling strategies

Risk Management

An organized, analytic process to identify what might cause harm or loss (i.e., identify risks); to assess and quantify the identified risks; and to develop and, if needed, implement an appropriate approach to prevent or handle causes of risk that could result in significant harm or loss

Risk Posture

A perspective of the level of risk faced by an entity or organization that is based on a prioritized inventory of current and anticipated risk exposures

Secure Coding

Development of software in a manner that reduces the probability of security vulnerabilities, such as defects, bugs, logic flaws and code anomalies

Security

Defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability of a system

Security/Resilience

Possessing the characteristics associated with not only the fundamentals of cybersecurity management, such as confidentiality, integrity, and availability, but also the broader adaptive proactive processes required to manage the evolving global cyber risk landscape (See *Security* and *Resilience*.)

Service

Activity that an entity or organization carries out in performing a duty or creating a product

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Service Continuity Plan

A service-specific plan for sustaining services and associated assets under degraded conditions

Situational Awareness

Awareness of the environment and its events to enable (1) active discovery and analysis of information related to immediate operational stability and security and (2) coordination of that information across the enterprise

Stakeholder

A person or organization that has a vested interest in the activities of the organization/program

Standard

A document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context

Supplier

An organization or individual that the acquirer utilizes to supply a product or service (This organization or individual includes all suppliers in the supply chain, developers or manufacturers of systems, system components, government, infrastructure, and third-party partners. These suppliers may rely on contracts or be non-contracted.)

Supplier Agreement

A formal or informal understanding, typically in the form of a document that outlines a seller promise to supply materials or services that an entity desires over a period of time for an established cost or exchange of resources

Supplier Transition Management

The act of managing changes over the lifecycle of a supplier relationship, typically beginning with establishing requirements, followed by an agreement/contract, and (at some point) a dissolution of that relationship and potentially the move to a new supplier

Third-Party Contractors

See *Supplier*.

Threat

The combination of a vulnerability, a threat actor, a motive (if the threat actor is a person or persons), and the potential to produce a harmful outcome for the acquirer

Threat Monitoring

The analysis, assessment, and review of audit trails and other information collected for the purpose of searching out events or exposures that may constitute risks to an entity

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Tradeoff Analysis

Analytical evaluation of design options/alternatives against performance, design-to-cost objectives, and lifecycle quality factors

Triggering Criteria (Triggering Events)

Characteristics or requirements that cause an entity, system, or program to initiate (i.e., trigger) one or more functional processes

Trusted Supplier (ICT)

A supplier that provides information and communications technology to the acquirer, which the acquirer has justifiable reason to believe meets appropriate standards for the intended use (A supplier can achieve this designation by demonstrating compliance with standards set forth by an acknowledged authority to ensure the integrity of the technology purchased.)

User Representatives

Individuals familiar with the requirements of a process or system who can offer input, guidance, and feedback in support of development, changes, or issue resolution

Validation

Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled

Vulnerability

A characteristic of design, location, security posture, operation, or any combination of these that renders an asset, system, network, or entity susceptible to disruption, destruction, or exploitation

Work Product

Artifact resulting from the execution of a process

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Bibliography

URLs are valid as of the publication date of this report.

[Alberts 2002]

Alberts, Christopher & Dorofee, Audrey. *Managing Information Security Risks: The OCTAVE Approach.* Addison-Wesley. 2002. ISBN 0321118863. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=30678

[Alberts 2014]

Alberts, Christopher; Woody, Carol; & Dorofee, Audrey. *Introduction to the Security Engineering Risk Analysis (SERA) Framework.* CMU/SEI-2014-TN-025. Software Engineering Institute, Carnegie Mellon University. 2014. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=427321

[Alberts 2017a]

Alberts, Christopher & Woody, Carol. *Prototype Software Assurance Framework (SAF): Introduction and Overview.* CMU/SEI-2017-TN-001. Software Engineering Institute, Carnegie Mellon University. 2017. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=496134

[Alberts 2017b]

Alberts, Christopher; Woody, Carol; Wallen, Charles; & Haller, John. Assessing DoD System Acquisition Supply Chain Risk Management. *CrossTalk*. Volume 30. Issue Number 3. May/June 2017. Page 4. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=499297

[Caralli 2010]

Caralli, Richard A.; Allen, Julia H.; & White, David W. *CERT Resilience Management Model: A Maturity Model (CERT-RMM) A Maturity Model for Managing Operational Resilience.* Addison-Wesley. 2010. ISBN 0321712439. https://www.informit.com/store/cert-resilience-management-model-cert-rmm-a-maturity-9780321712431

[Chrissis 2006]

Chrissis, Mary Beth; Konrad, Mike; & Shrum, Sandy. *CMMI: Guidelines for Process Integration and Product Improvement, Third Edition*. Addison-Wesley. 2006. ISBN 9812382380. https://www.informit.com/store/cmmi-for-development-guidelines-for-process-integration-9780132700467

[DHS 2014]

Department of Homeland Security (DHS). Assessments: Cyber Resilience Review (CRR). *Cybersecurity and Infrastructure Security Agency (CISA)*. October 19, 2022 [accessed]. https://www.us-cert.gov/ccubedvp/self-service-crr

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

[Dorofee 1996]

Dorofee, Audrey; Walker, Julie; Alberts, Christopher; Higuera, Ron; Murphy, Richard; & Williams, Ray. *Continuous Risk Management Guidebook.* Software Engineering Institute, Carnegie Mellon University. 1996. ISBN 0967260108. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=30856

[Dvorak 2009]

Dvorak, Daniel L., ed. *NASA Study on Flight Software Complexity*. National Aeronautics and Space Administration (NASA) Systems and Software Division, Jet Propulsion Laboratory, California Institute of Technology. 2009.
http://www.nasa.gov/pdf/418878main_FSWC_Final_Report.pdf

[Ferguson 1996]

Ferguson, Jack; Cooper, Jack; Falat, Michael; Fisher, Matt; Guido, Anthony; Marciniak, John; Matejceck, Jordan; & Webster, Robert. *Software Acquisition Capability Maturity Model (SA-CMM) Version 1.03*. CMU/SEI-96-TR-020. Software Engineering Institute, Carnegie Mellon University. 1996. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6099

[ISO/IEC 2021]

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). *Cybersecurity—Supplier Relationships—Part 1: Overview and Concepts*. ISO/IEC 27036-1:2021. ISO/IEC. 2021. https://www.iso.org/standard/82905.html

[ISO/IEC 2022a]

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). *Cybersecurity—Supplier Relationships—Part 2: Requirements*. ISO/IEC 27036-2:2022. ISO/IEC. 2022. https://www.iso.org/standard/82060.html

[ISO/IEC 2022b]

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). *Cybersecurity—Supplier Relationships—Part 3: Guidelines for Hardware, Software, and Services Supply Chain Security*. ISO/IEC DIS 27036-3. ISO/IEC. 2022 [accessed/in progress]. https://www.iso.org/standard/82890.html

[ISO/IEC/IEEE 2017]

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). *Systems and software engineering — Vocabulary.* ISO/IEC/IEEE 24765:2017. 2017. https://www.iso.org/standard/71952.html

[ISO/TC 2022]

International Organization for Standardization/Technical Committee (ISO/TC). *Security and Resilience—Security Management Systems—Requirements*. ISO 28000:2022. ISO/TC. 2022. https://www.iso.org/standard/79612.html

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

[Mainstay 2010]
Mainstay Partners, LLC. *Does Application Security Pay? Measuring the Business Impact of Software Security Assurance Solutions.* Mainstay. 2010. https://www.mainstay-company.com/PDF/Fortify%20WP%20for%20print-F2%20-%20page8.pdf

[Microsoft 2014]
Microsoft Corporation. *Benefits of the SDL.* September 2014. https://www.microsoft.com/en-us/securityengineering/sdl

[NIA 2010]
Committee on National Security Systems. *National Information Assurance (IA) Glossary CNSS Instruction*. CNSS Instruction No. 4009. 2010.
https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf

[NIST 2002]
National Institute of Standards and Technology (NIST). *Risk Management Guide for Information Technology Systems*. NIST SP 800-30, Revision 1. NIST Computer Security Resource Center (CSRC). 2002. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

[NIST 2011]
National Institute of Standards and Technology (NIST). *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST SP 800-39. NIST Computer Security Resource Center (CSRC). 2011. https://csrc.nist.gov/publications/detail/sp/800-39/final

[NIST 2018]
National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. NIST CSWP 6. NIST Computer Security Resource Center (CSRC). 2018. https://csrc.nist.gov/publications/detail/white-paper/2018/04/16/cybersecurity-framework-v11/final

[NIST 2022]
National Institute of Standards and Technology (NIST). *Glossary*. September 2022.
https://csrc.nist.gov/glossary

[Paulk 1993]
Paulk, Mark; Curtis, Bill; Chrissis, Mary Beth; & Weber, Charlie. *Capability Maturity Model for Software, Version 1.1.* CMU/SEI-93-TR-024. Software Engineering Institute, Carnegie Mellon University. 1993. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=11955

[Soo Hoo 2001]
Soo Hoo, K.; Sudbury, A. W.; & Jaquith, A. R. Tangible ROI Through Secure Software Engineering. *Secure Business Quarterly.* Volume 1. Issue 2. Fourth Quarter, 2001.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

[U.S. Code 2013]
One Hundred Twelfth Congress of the United States of America. *National Defense Authorization Act for Fiscal Year 2013*. H.R. 4310. Public Law No: 112-239. U.S. Government Publishing Office. 2013. http://www.gpo.gov/fdsys/pkg/BILLS-112hr4310enr/pdf/BILLS-112hr4310enr.pdf

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. **AGENCY USE ONLY**
(Leave Blank)

2. **REPORT DATE**
October 2022

3. **REPORT TYPE AND DATES COVERED**
Final

4. **TITLE AND SUBTITLE**
Acquisition Security Framework (ASF): Managing Systems Cybersecurity Risk

5. **FUNDING NUMBERS**
FA8702-15-D-0002

6. **AUTHOR(S)**
Christopher Alberts, Michael Bandor, Charles M. Wallen, & Carol Woody

7. **PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. **PERFORMING ORGANIZATION REPORT NUMBER**
CMU/SEI-2022-TN-003

9. **SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

10. **SPONSORING/MONITORING AGENCY REPORT NUMBER**
n/a

11. **SUPPLEMENTARY NOTES**

12A **DISTRIBUTION/AVAILABILITY STATEMENT**
Unclassified/Unlimited, DTIC, NTIS

12B **DISTRIBUTION CODE**

13. **ABSTRACT (MAXIMUM 200 WORDS)**

The Acquisition Security Framework (ASF) is a collection of leading practices for building and operating secure and resilient software-reliant systems across the systems lifecycle. It enables programs to evaluate risks and gaps in their processes for acquiring, engineering, and deploying secure software-reliant systems and provides programs more insight and control over their supply chains. The ASF provides a roadmap for building security and resilience into a system rather than “bolting them on” after deployment. The framework is designed to help programs coordinate the management of engineering and supply chain risks across the many components of a system, including hardware, network interfaces, software interfaces, and mission capabilities. ASF practices promote proactive dialogue across all program and supplier teams, helping to integrate communications channels and facilitate information sharing. The framework is consistent with cybersecurity engineering, supply chain management, and risk management guidance from the International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), and Department of Homeland Security (DHS). This report presents an overview of the ASF and its development status. It also includes a snapshot of the practices that have been developed so far and outlines a plan for completing the ASF body of work.

14. **SUBJECT TERMS**
Acquisition Security Framework, ASF, resiliency, software-reliant systems

15. **NUMBER OF PAGES**
82

16. **PRICE CODE**

17. **SECURITY CLASSIFICATION OF REPORT**
Unclassified

18. **SECURITY CLASSIFICATION OF THIS PAGE**
Unclassified

19. **SECURITY CLASSIFICATION OF ABSTRACT**
Unclassified

20. **LIMITATION OF ABSTRACT**
UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18 298-102

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.