**NIST Special Publication 800-160**

**Initial Public Draft**

# Systems Security Engineering

*An Integrated Approach to Building Trustworthy Resilient Systems*

**RON ROSS**
**JANET CARRIER OREN**
**MICHAEL McEVILLEY**

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

**NIST Special Publication 800-160**

**Initial Public Draft**

# Systems Security Engineering

*An Integrated Approach to Building Trustworthy Resilient Systems*

**RON ROSS**
*Computer Security Division*
*National Institute of Standards and Technology*

**JANET CARRIER OREN**
*Information Assurance Directorate*
*National Security Agency*

**MICHAEL McEVILLEY**
*Center for National Security*
*The MITRE Corporation*

**May 2014**


U.S. Department of Commerce
*Penny Pritzker, Secretary*

National Institute of Standards and Technology
*Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director*

## Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

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

National Institute of Standards and Technology Special Publication 800-160
**121 pages** (May 2014)

CODEN: NSPUE2

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

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

Organizations are encouraged to review draft publications during the designated public comment periods and provide feedback to NIST. Computer Security Division publications are available at **http://csrc.nist.gov/publications**.

**Public comment period: May 13 through July 11, 2014**
**Comments on this publication may be submitted to:**

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

## Reports on Computer Systems Technology

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

## Abstract

This publication addresses the engineering-driven actions necessary for developing a more defensible and survivable information technology (IT) infrastructure—including the component products, systems, and services that compose the infrastructure. It starts with and builds upon a set of well-established International Standards for systems and software engineering published by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the Institute of Electrical and Electronic Engineers (IEEE) and infuses systems security engineering techniques, methods, and practices into those systems and software engineering processes. The ultimate objective is to address security issues from a stakeholder requirements and protection needs perspective and to use established organizational processes to ensure that such requirements and needs are addressed early in and throughout the life cycle of the system.

## Keywords

Systems engineering, systems security engineering, assurance, trustworthiness, information security, information security policy, security architecture, security design, system life cycle, verification, validation, disposal, integration, implementation, stakeholder, security requirements, protection needs, resiliency, requirements analysis, risk management, risk assessment, risk treatment, security authorization, engineering trades, systems, system-of-systems, system element, system component, penetration testing, inspection, review, developmental engineering, field engineering, specifications.

## Acknowledgements

The authors gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication. The authors also respectfully acknowledge the seminal work in computer and information security that dates back to the 1960s. The vision, insights, and dedicated efforts of the early pioneers in computer security serve as the philosophical and technical foundation for the concepts, principles, and practices employed in this publication to address the problem of engineering secure systems.

## Notes to Reviewers

NIST Special Publication 800-160 represents a comprehensive two-year interagency initiative to define systems security engineering processes that are tightly coupled to and fully integrated into well-established, international standards-based systems and software engineering processes. The project supports the federal cyber security strategy of "*Build It Right, Continuously Monitor*" and consists of a *four-phase* development approach that will culminate in the publication of the final systems security engineering guideline at the end of 2014. The four phases include:

- **Phase 1:** Development of the systems security engineering *technical processes* based on the technical systems and software engineering processes defined in ISO/IEC/IEEE 15288:2008;
- **Phase 2:** Development of the remaining supporting appendices (i.e., Information Security Risk Management (including the integration of the Risk Management Framework [RMF], security controls, and other security- and risk-related concepts into the systems security engineering processes), Use Case Scenarios, Roles and Responsibilities, System Resiliency, Security and Trustworthiness, Acquisition Considerations, and the Department of Defense Systems Engineering Process (Summer 2014);
- **Phase 3:** Development of the systems security engineering *nontechnical processes* based on the nontechnical systems and software engineering processes (i.e., Agreement, Organizational Project-Enabling, and Project) defined in ISO/IEC/IEEE 15288: 2008 (Fall 2014); and
- **Phase 4:** Alignment of the technical and nontechnical processes based on the updated systems and software engineering processes defined in ISO/IEC/IEEE DIS 15288:201x(E) (Fall or Winter 2014 subject to the final publication schedule of the international standards bodies).

Since there are many stakeholders involved in the systems engineering and the systems security engineering processes and those processes are relatively complex, the phased-development approach of Special Publication 800-160 will allow reviewers to focus on key aspects of the engineering processes and to provide their feedback for those sections of the publication as they are developed and released for public review.

The full integration of the systems security engineering discipline into the systems and software engineering discipline involves fundamental changes in the traditional ways of doing business within organizations—breaking down institutional barriers that over time, have isolated security activities from the mainstream organizational management and technical processes including, for example, the system development life cycle, acquisition/procurement, and enterprise architecture. The integration of these interdisciplinary activities requires the strong support of senior leaders and executives and increased levels of communication among all stakeholders who have an interest in, or are affected by, the systems being developed or enhanced.

Your feedback to us, as always, is important. We appreciate each and every contribution from our reviewers. The very insightful comments from both the public and private sectors, nationally and internationally, continue to help shape our publications and ensure that they are meeting the needs and expectations of our customers.

-- RON ROSS
JOINT TASK FORCE LEADER
FISMA IMPLEMENTATION PROJECT LEADER

***Disclaimer***

The material contained in this publication is intended to be used solely as a supplement to and in conjunction with International Standards **ISO/IEC/IEEE 15288** *Systems and software engineering—System life cycle processes*. Copies of the above standards can be obtained from the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), or the Institute of Electrical and Electronic Engineers (IEEE) at: **http://www.iso.org**; **http://www.iec.ch**; or **http://ieee.org**, respectively.

# Table of Contents

## Prologue

"*…Through the process of risk management, leaders must consider risk to US interests from adversaries using cyberspace to their advantage and from our own efforts to employ the global nature of cyberspace to achieve objectives in military, intelligence, and business operations… "*

*"…For operational plans development, the combination of threats, vulnerabilities, and impacts must be evaluated in order to identify important trends and decide where effort should be applied to eliminate or reduce threat capabilities; eliminate or reduce vulnerabilities; and assess, coordinate, and deconflict all cyberspace operations…"*

*"…Leaders at all levels are accountable for ensuring readiness and security to the same degree as in any other domain…"*

-- THE NATIONAL STRATEGY FOR CYBERSPACE OPERATIONS
OFFICE OF THE CHAIRMAN, JOINT CHIEFS OF STAFF, U.S. DEPARTMENT OF DEFENSE

## Foreword

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

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

The Task Force stated that the susceptibility to the advanced cyber threat by the Department of Defense is also a concern for public and private networks, in general, and recommended that steps be taken immediately to build an effective response to measurably increase confidence in the IT systems we depend on (public and private) and at the same time, decrease a would-be attacker's confidence in the effectiveness of their capabilities to compromise our systems. This conclusion was based upon: (i) the success adversaries have had penetrating our networks; (ii) the relative ease that our Red Teams have in disrupting, or completely beating, our forces in exercises using exploits available on the Internet; and (iii) the weak cyber hygiene position of our networks and systems.

The Task Force also described several classes of vulnerabilities within organizations: (i) *known vulnerabilities* (characterized by ongoing patching operations); (ii) *unknown vulnerabilities* (the subject of zero-day exploits or attacks); and (iii) *adversary-created vulnerabilities* (the subject of the advanced persistent threat). The important message from the Defense Science Board is that two out the three classes of vulnerabilities (the unknown vulnerabilities and adversary-created vulnerabilities) are totally invisible to most organizations. These types of vulnerabilities can only be addressed by sound architectural and engineering techniques, methodologies, and practices—in essence, providing the penetration resistance, trustworthiness, and resilience to withstand sophisticated, well-resourced cyber attacks on the systems supporting critical missions and business operations. To begin to address the significant cybersecurity challenges of the 21st century, we must—

- Understand the modern *threat* space (including the capabilities, intentions, and targeting actions of adversaries);
- Identify and segregate *critical assets* within our enterprises;
- Reduce and manage the growing *complexity* of our systems and networks that are the nerve centers of our IT infrastructure;
- Use *security requirements* derived from mission/business protection needs to drive the integration of *security functions* and *security services* into the mainstream management and technical processes within our enterprises;[1] and

[1] Mainstream processes include, for example: enterprise architecture; system life cycle; systems engineering; and acquisition/procurement.

- Develop more *penetration-resistant*, *trustworthy*, and *resilient* systems that are capable of supporting critical missions and business operations with a level of assurance or confidence that is consistent with the risk tolerance of the organization.

This publication addresses the actions necessary for developing a more defensible and survivable information technology (IT) infrastructure—including the component products, systems, and services that compose the infrastructure. It starts with and builds upon a set of well-established International Standards for systems and software engineering published by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the Institute of Electrical and Electronic Engineers (IEEE) and infuses systems security engineering techniques, methods, and practices into those systems and software engineering processes. The ultimate objective is to address security issues from a stakeholder requirements and protection needs perspective and to use established organizational processes to ensure that such requirements and needs are addressed early in and throughout the life cycle of the system.

Recognizing that increasing the trustworthiness and resiliency of the IT infrastructure is a significant undertaking that requires a substantial investment in the architectural design and development of our systems and networks, introducing a disciplined, structured, and standards-based set of systems security engineering processes can provide an important starting point and forcing function to initiate needed change.

-- Ron Ross
**National Institute of Standards and Technology**

CHAPTER ONE

# INTRODUCTION

THE NEED FOR MORE TRUSTWORTHY AND RESILIENT SYSTEMS

Today, more than at any time in history, individuals, groups, and organizations rely on advanced *technology*[2] to carry out a wide range of missions and business functions. The complete reliance on advanced technology means that the systems[3] developed and deployed to support federal applications and operations must be dependable despite a growing set of threats including, for example, hostile attacks, natural disasters, structural/component failures, and errors of omission and commission. To help ensure that organizations can carry out their mission and business responsibilities in these threat-laden environments, all systems must possess adequate protection capability. The effects of sophisticated and well-orchestrated cyber attacks that are part of the *advanced persistent threat*,[4] for example, can be minimized if not completely defeated by the application of the principles, concepts, and techniques representing the best practices upon which the systems security engineering processes are based. Since it is impossible to know of all possible threats and to stop all anticipated threats, the architectural design of systems must be inherently less susceptible to such threats, provide an increased level of penetration resistance, and also provide engineered-in resiliency—so missions and business functions can continue even when systems are operating in degraded or debilitated states.

The derived value of any engineering discipline is to first have a well-informed understanding of the problem to be solved. To maximize the effects of systems security engineering processes, security requirements that specify the protection needs required of the security functions and mechanisms needed to protect systems from such threats, must be considered *first-order* requirements and cannot be added on after the fact. Rather, the protection capability must be built in and tightly integrated into the systems as part of the system life cycle process. Therefore, understanding the protection capability need and expressing that need through well-defined security requirements becomes an important enterprise *investment* in mission/business success in the modern age of global commerce and network connectivity.

This document defines *systems security engineering* as a specialty discipline of systems engineering. It also provides a description of the processes, activities, and tasks performed by systems security engineering professionals. Systems security engineering contributes to a holistic security perspective and focus within the engineering efforts to ensure that mission and business

[2] The term *technology* is used in the broadest context in this publication to include information, communications, and computing technologies as well as any mechanical, hydraulic, or pneumatic components in systems that contain or are enabled by such technologies. This view of technology provides an increased visibility and recognition of the digital computational foundation of modern complex systems and the importance of the trustworthiness of that foundation in providing the system's core functional capability.

[3] Systems include, for example: general purpose information systems; industrial/process control systems; weapons systems; environmental control systems; and command, control, and communications systems. These systems can be found in a variety of sectors such as national defense, financial, transportation, manufacturing, healthcare, and energy. All uses of the term *system* include the personnel that interact with the system to achieve the mission or business objectives.

[4] The advanced persistent threat is an adversary possessing sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the IT infrastructure of the targeted organizations for purposes of exfiltrating information, undermining/impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future.

risk concerns that result from the operation and use of systems deployed by organizations, are properly identified and addressed in all systems engineering tasks. Systems security engineering activities draw on well-established security principles, concepts, and techniques to leverage, adapt, and supplement the relevant principles and practices of systems engineering. Such activities are performed consistently at every stage of the system life cycle, including the concept stage, development stage, production stage, utilization/support stages, and retirement—thus enabling delivery of trustworthy, resilient systems that satisfy stakeholder[5] requirements and enforce the organizational security policies within the constraints[6] and risk tolerance defined by the stakeholders.

***Engineering to Reduce Susceptibility to Threats***

One of the important objectives of systems security engineering is to reduce *susceptibility* to *threats*. Such reduction is achieved by smart *architectural design*, which in a world of constantly changing threats and an increasingly large number of unknown vulnerabilities, limits exposure, contains damage, and provides the basis to react and recover from failure—to include failure resulting from malicious activity.

## 1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is fivefold: (i) to provide a comprehensive statement of the systems security engineering discipline, its principles, concepts, and activities; (ii) to foster a common mindset to deliver security for any system, regardless of its scope, size, complexity, or stage of the system life cycle; (iii) to advance the field of systems security engineering by promulgating it as a discipline that can be applied and studied; (iv) to demonstrate how systems security engineering processes can be effectively integrated into systems engineering processes; and (v) to serve as a basis for the development of educational and training programs, including the development of individual certifications and other professional assessment criteria.

The systems security engineering discipline is applicable at each stage of the system life cycle and can be employed to deliver protection capability as part of the following types of systems:

- New systems. The engineering effort includes such activities as preliminary/applied research to refine concepts and technologies employed in a new system. This effort is initiated during the development/acquisition stage of the system life cycle.
- Planned upgrades to fielded systems while continuing to sustain day-to-day operations. The planned system upgrades may enhance an existing system capability, provide a new capability, or constitute a technology refresh of an existing capability. This effort occurs during the operation/maintenance stage of the system life cycle.

[5] A *stakeholder* is a person, group, or organization (or designated representative for a person, group, or organization) that has a direct or indirect interest in a system because that person, group, or organization can affect or be affected by the objectives, policies, or operations related to the system at any stage of the life cycle. The backgrounds, expertise, and roles of the stakeholders can include a range of specialties, responsibilities, and influences on the system. Some stakeholders are identified as *key stakeholders* for some or all of the processes. The key stakeholders are individuals with decision-making authority relevant to the mission/business and to the systems supporting the mission/business.

[6] The engineering team has a responsibility to help stakeholders define all relevant constraints so that those constraints may be transformed into engineering requirements.

- Reactive modifications to fielded systems. The engineering effort occurs in response to threats such as cyber attacks, incidents, errors, accidents, faults, structural/component failures, and natural disasters that diminish or prevent the system from achieving its original design intent. The effort occurs during the operations/maintenance stage of the system life cycle and may be performed concurrently with or independent of day-to-day operations/maintenance.
- Planned upgrades to fielded systems that result in new systems. The engineering effort is carried out as if developing a new system with a system life cycle that is distinct from the life cycle of a fielded system. Upgrades are performed in a development environment, independent of the fielded system.
- System-of-systems. The engineering effort occurs across a set of constituent systems, each with its own primary purpose and planned evolution. The composition of the constituent systems into a system-of-systems produces a capability that would otherwise be more difficult or impractical to achieve. This effort can occur across a continuum—from an informal, unplanned system-of-systems concept and evolution that emerges over time via voluntary participation, to degrees of more formal execution with the most formal being a system-of-systems concept that is directed, planned, structured, and achieved via a centrally managed, collaborative engineering effort.
- Retirement of all or portions of fielded systems. The engineering effort removes a system from operation and may also include the transition of system operations to some other system or systems. The effort occurs during the disposal/retirement stage of the system life cycle and may have to be carried out while sustaining day-to-day operations.

## 1.2 TARGET AUDIENCE

This publication is intended for security professionals who are responsible for the activities and tasks that are defined by the systems security engineering processes described in Chapter Three. The term *systems security engineer* is used to include those security professionals who perform any or all of the activities and tasks defined by the systems security engineering processes. The term may apply to an individual or a team of individuals from the same organization or different organizations. This publication can also be used by professionals who perform other system life cycle activities, allowing those individuals to acquire an understanding of the systems security engineering processes. These include:

- Individuals with governance, risk management, security, and oversight responsibilities;
- Individuals with acquisition, budgeting, and project management responsibilities;
- Individuals with system design, development, and integration responsibilities;
- Individuals with system security, operations, sustainment, and support responsibilities;
- Individuals with independent verification and validation, testing/evaluation, auditing, security assessment, inspections, and monitoring responsibilities; and
- Providers of technology products, systems, or services.

## 1.3 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the systems security engineering discipline and the fundamental security principles, concepts, and terminology that provide the underlying technical and scientific basis for the systems security engineering processes.

- **Chapter Three** describes the systems security engineering processes as extensions to the systems engineering processes defined in the international systems and software engineering standards ISO/IEC/IEEE 15288. Each of the eleven systems engineering processes[7] contains a specific set of security enhancements that augment/extend the process outcomes, activities, and tasks defined by the international standards. The enhanced engineering processes address system security at every stage of the system life cycle.[8]
- **Supporting appendices** provide additional information for the systems security engineering processes including: (i) general references; (ii) definitions and terms; (iii) acronyms; (iv) a summary of the activities and tasks that compose the systems security engineering processes; (v) a description of information security risk management principles and concepts and how those principles and concepts relate to the systems security engineering processes; (vi) use case scenarios illustrating how to apply systems security engineering to systems engineering processes to deliver systems in different circumstances throughout the system life cycle; (vii) roles and responsibilities of individuals that are directly or indirectly involved in the systems security engineering processes; (viii) a primer on security and trustworthiness; (ix) how system resiliency techniques and concepts are applied in the systems security engineering processes; (x) systems security engineering processes as applied to Department of Defense applications and systems; and (xi) acquisition and procurement considerations for systems security engineering.

***The Power of Science and Engineering***

When we drive across a bridge, we generally have an *expectation* that the bridge we are crossing will not collapse and will get us to our destination without incident. For bridge builders, it's all about *physics*—equilibrium, static and dynamic loads, vibrations, and resonance. The science of physics combines with sound civil engineering techniques to produce a final product in which the general public has high confidence. For system developers, there are very similar fundamental principles in *mathematics*, *computer science*, and *systems/software engineering*, that when properly employed, provide the necessary and sufficient penetration resistance, trustworthiness, strength of mechanism, and resilience to give individuals that same level of confidence when driving across a bridge. Sufficiently secure systems cannot be achieved by good cyber hygiene activities alone. Rather, it will take a significant investment in strengthening the underlying information technology infrastructure by initiating systems engineering efforts driven by security architectures and security designs that have been proven to produce sound engineering-based solutions to complex and challenging security problems.

[7] Future versions of this publication will address the security aspects of the fourteen nontechnical processes described in the ISO/IEC/IEEE 15288.

[8] While there are a variety of system life cycle processes in use today, this publication, by convention, uses the systems engineering life cycle stages of: concept; development; production; utilization; support; and retirement.

CHAPTER TWO

# THE FUNDAMENTALS

SECURITY PRINCIPLES AND CONCEPTS USED IN SYSTEMS SECURITY ENGINEERING

This chapter: (i) defines the discipline of systems security engineering and its relationship to systems engineering; (ii) discusses the systems security engineering view of systems and system elements; and (iii) discusses the foundational concepts, principles, and best practices that provide the basis for the contributions that systems security engineering makes to systems engineering. Understanding the foundational security concepts, principles, and best practices and how those concepts, principles, and practices can be seamlessly applied to and integrated within a comprehensive systems engineering effort, is important for organizations desiring to fundamentally increase the trustworthiness and resiliency of the systems they deploy in support of mission/business operations. The ultimate objective is to have security-related activities (driven by organizational culture and mindset) tightly integrated into the mainstream technical and management processes within organizations.[9] The most effective organizations with regard to the protection of organizational assets proactively consider security as an investment in mission/business success—not as a separate activity or programmatic element disconnected from the mission/business context and operational requirements.

## 2.1 SYSTEMS SECURITY ENGINEERING

Systems security engineering is a specialty engineering discipline of systems engineering. The discipline applies scientific, mathematical, engineering, and measurement concepts, principles, and methods to deliver, consistent with defined constraints and necessary trade-offs, a trustworthy asset protection capability that: (i) satisfies stakeholder requirements; (ii) is capable of enforcing an organizational security policy; (iii) is seamlessly integrated into the delivered system; and (iv) presents residual risk that is deemed acceptable and manageable to stakeholders. As part of a comprehensive systems engineering effort, systems security engineering:

- Assesses susceptibility to threats in the projected or actual environment of operation;
- Identifies and assesses vulnerabilities in a system and its environment of operation;
- Identifies, specifies, designs, and develops protective measures[10] to address system vulnerabilities;
- Identifies and evaluates protective measures to ascertain their suitability, effectiveness and degree to which they can be expected to reduce mission/business risk;
- Provides assurance evidence to substantiate the trustworthiness of protective measures;
- Identifies, quantifies, and evaluates the costs and benefits of protective measures to inform engineering trade-off and risk treatment decisions; and

[9] Mainstream organizational processes include, for example, enterprise architecture, acquisition/procurement processes, system life cycle processes, and systems engineering processes.

[10] Protective measures (also referred to as protections) are the safeguards, countermeasures, and techniques employed to: (i) design and implement trustworthy systems with inherent protection capabilities; and (ii) mitigate risk, where necessary. Protective measures are implemented in hardware, software, and firmware mechanisms; physical and structural components; and by procedural means.

- Leverages multiple security focus areas to ensure that protective measures are appropriate, effective in combination, and interact properly with other system capabilities.[11]

Systems security engineering includes a combination of technical and nontechnical activities. These activities are based on foundational security concepts, principles, and best practices and are intended to provide substantiated confidence that protective measures function only as specified, enforce security policy, produce the desired outcome, and warrant the trustworthiness required by stakeholders. Systems security engineering activities are intended to be performed throughout every stage of the system life cycle. Systems security engineering views security: (i) as a protection capability that satisfies security requirements and is delivered as part of the system; and (ii) as a quality property of the entire delivered system when it is properly configured and used to enforce the security policy associated with mission/business operations. It is the need to satisfy security requirements and to enforce a security policy that differentiates systems security engineering from other systems engineering specialties. A sufficiently trustworthy system results from adherence to the security concepts, principles, and practices in the application of security-specific methods, techniques, and analyses, some of which stand alone and others that supplement existing systems engineering techniques, methods, and analyses.[12]

There are four areas in which systems security engineering adds value and contributes to general systems engineering processes. These include: (i) *protection needs*; (ii) *security relevance*; (iii) *trustworthiness* and *assurance*; and (iv) *security risk management*. These areas guide all systems security engineering activities, tasks, and outcomes.

- Protection Needs. Protection needs provide the appropriate scope for the engineering effort and influence the identification, selection, and employment of protective measures. Protective measures represent the security-relevant portions of the system and the security-relevant aspects of the systems engineering effort. Protection needs are determined: (i) for all types of mission/business assets; (ii) for all system-level assets necessary for the secure execution, management, and self-protection of the system; and (iii) as dictated by engineering and risk treatment trade decisions. Protection needs are continuously reassessed and adjusted as the system design and concept of operation mature or as threats and vulnerabilities are identified.
- Security Relevance. Security-relevant elements of the system are the focus of systems security engineering activities. Being able to differentiate between what is and what is not security-relevant is the basis for all forms of security analyses and underlies security architectural design and composing a secure system from its security-relevant components. The security-relevant elements of a system are relied upon to enforce security policy and exhibit predictable behavior while delivering the specified protection capability, despite being subjected to: malicious attack; accidental or incidental misuse; human error of omission and commission; component faults and failures; or man-made or natural disasters.
- Trustworthiness and Assurance. The trustworthiness of a system is determined from the assurance/confidence that the system is adequate to provide the specified protections and enforce the security policy, given its intended use.

[11] Security focus areas include, for example: computer security; communications security; transmission security; operational security; anti-tamper protection; electronic emissions security; information, software, and hardware assurance; as well as technology specialties (e.g., biometrics, cryptographic).

[12] Safety, reliability, and fault tolerance each have constructs and techniques that are shared with security. However, the application of those constructs and techniques to achieve safety, reliability, and fault tolerance does not necessarily achieve security.

- Security Risk Management. Security risk originates from the inherent vulnerabilities in the system and the vulnerabilities associated with the intended use of the system, given the potential threats in the environment of operation and the missions/business functions supported by the system. Security risk management activities strive to constrain risk to a manageable level throughout the system life cycle. Systems security engineering risk management activities develop and execute plans to identify, prioritize, and treat (i.e., respond to) risk to the degree possible within the scope of control of the engineering effort, and within the constraints and priorities specified by stakeholders.[13]

Figure 1 illustrates the essential contributions of the systems security engineering discipline to systems engineering.

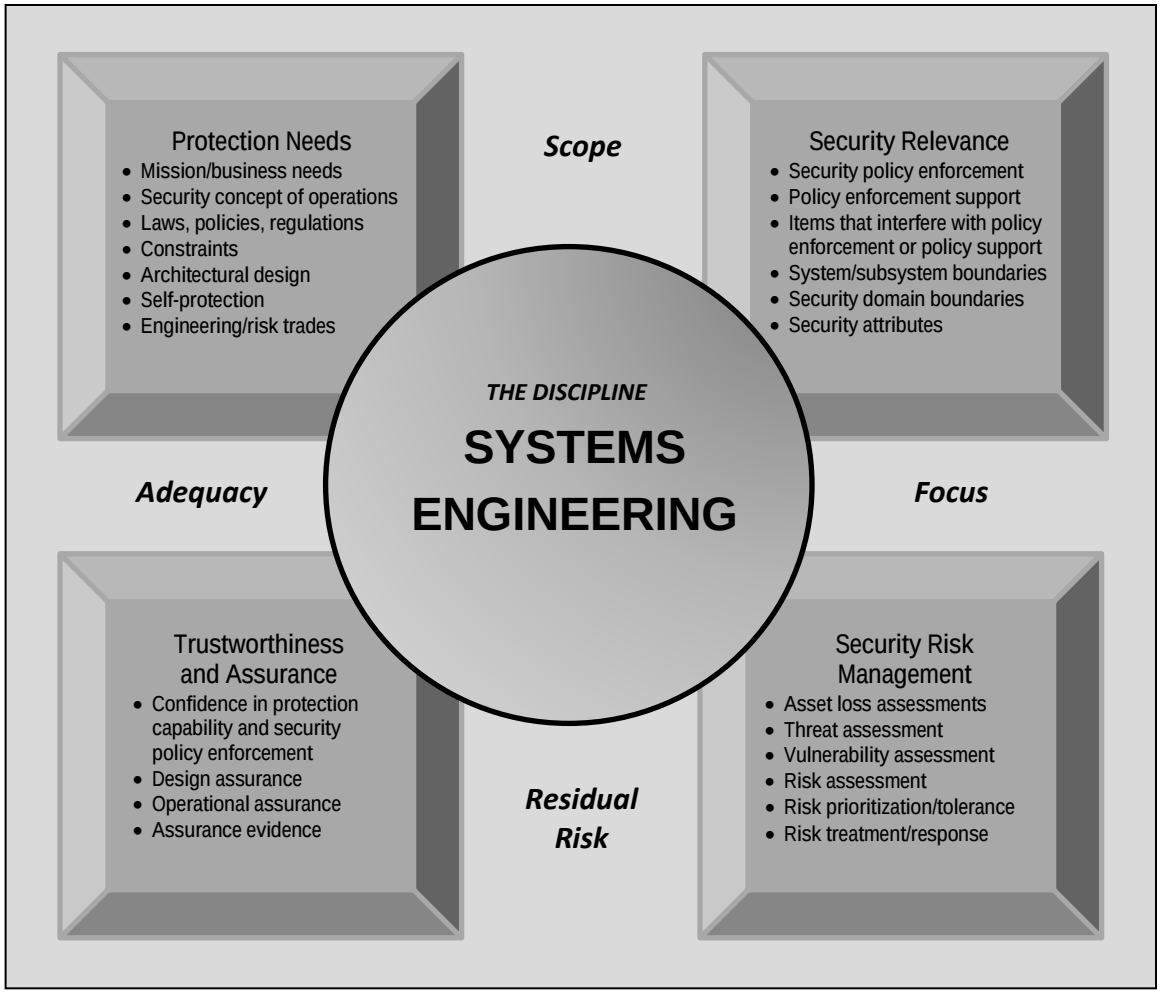


**FIGURE 1: ESSENTIAL CONTRIBUTIONS OF SYSTEMS SECURITY ENGINEERING**

[13] Security risk management is one of the systems engineering life cycle processes. The risk management activities associated with the systems security engineering processes is only that portion of managing risk that occurs during the engineering effort and only within the scope of control of that effort. Once the system is delivered, the operations and sustainment organization is responsible for managing the delivered risk (i.e., the residual risk that was not sufficiently mitigated or eliminated during the systems engineering effort). NIST Special Publications 800-37 and 800-39 address the concept of information security risk management from the organization-level, mission/business process-level and the information system-level.

### *2.1.1 Role and Responsibility of the Systems Security Engineer*

The role of a systems security engineer is to participate in a multidisciplinary systems engineering team, applying fundamental systems security understanding, skills, expertise, and experience to develop a system that satisfies stakeholder mission/business requirements.[14] The systems security engineer is expected to have expertise and experience in multiple areas (e.g., protection needs assessment, requirements elicitation, security architecture, threat assessment, computer security, communication security, networking, security technologies, hardware and software development, test and evaluation, vulnerability assessment, penetration testing, and supply chain risk). Systems security engineer responsibilities include:

- Maintaining a comprehensive and holistic system view while addressing stakeholder security and risk concerns;
- Ensuring the effectiveness and suitability of the security elements of the system as an enabler to mission/business success;
- Ensuring that relevant threat and vulnerability data is considered in support of security-relevant decisions;
- Providing input to analyses of alternatives and to requirements, engineering, and risk trade-off analyses to achieve a cost-effective security architectural design for protections that enable mission/business success;
- Providing the evidence necessary to support assurance claims and to substantiate the determination that the system is sufficiently trustworthy; and
- Conducting security risk management activities, producing related security risk management information, and advising the engineering team and key stakeholders on the security-relevant impact of threats and vulnerabilities to the mission/business supported by the system.

The systems security engineer has a foundational understanding of systems engineering, to include the processes and roles for which the systems engineer is responsible. This understanding is necessary for effective participation on a systems engineering team. However, it is imperative in cases where systems security engineering activities are conducted in the absence of a systems engineering effort. This situation can occur at any stage in the system life cycle and may require the systems security engineer to assume additional responsibilities to ensure that the broader systems engineering concerns are identified and communicated to key stakeholders for action or resolution.

A systems security engineer may serve as the lead systems security engineer with responsibility for all systems security engineering activities reporting directly to the systems engineering team lead.[15] A systems security engineer may also participate as a member of a focused sub-team or to direct the systems security activities within a focused sub-team (e.g., an integrated product team). Finally, a systems security engineer may, in certain situations, serve as a consultant to another systems engineering team, providing security-relevant subject matter expertise in support of the team's engineering efforts.

[14] The size of the systems engineering team is determined by factors such as scope, size, duration, and complexity of the engineering effort. As the size of the team increases, there may be multiple sub-teams with clearly defined scopes and responsibilities. Typically, each sub-team has a leader. Ultimately, one individual assumes responsibility for the entire engineering effort. That individual may be referred to as the lead or chief systems engineer.

[15] Where the solution is a security system, the systems security engineer may serve as both the lead engineer and lead systems security engineer.

There are cases where a systems security engineer may participate on or provide consultation to teams performing system life cycle processes and activities that are not part of the developmental or field/sustainment engineering effort. Participation in such activities is best conducted under direction of management authority that is separate from that of the engineering effort to prevent conflict-of-interest concerns. Examples of teams that may be supported by a systems security engineer include:

- Independent Verification and Validation, Assessment, Audit, Certification, Test and Evaluation. This team employs independent system testing and evaluation to make recommendations about the suitability, sufficiency, effectiveness, and vulnerability of a system relative to its support to achievement of mission/business objectives.
- Security Authorization, System Approval to Operate/Connect, Engineering Project Milestone Decision. This team determines residual risk to the mission/business based on the engineering effort and the projected use of the system and makes recommendations to senior leaders regarding the acceptability of such risk in support of the system/security authorization process or approvals to operate/connect.[16] The team may also support decisions regarding preparedness of the engineering effort to proceed beyond a formal milestone in the system life cycle or acquisition life cycle process.
- Organizational Security Risk Management. This team provides security-related information to senior leaders across the organization to assist those leaders in managing the spectrum of mission/business risk at the organizational level, the mission/business process level, and the system level.[17]

Systems security engineers interact with a variety of stakeholders throughout the system life cycle. Stakeholders and their roles and responsibilities related to the engineering effort are identified at the start of a systems security engineering effort. Stakeholder roles/responsibilities may vary over the course of the systems engineering technical and management processes. Systems security engineers are capable of communicating with stakeholders at various levels of abstraction and in a variety of contexts—for example: (i) using high-level mission/business terms understood by senior executives; (ii) using more detailed technical terms understood by scientists and engineers; and (iii) using management terms understood by program/project managers. The systems security engineer builds strong relationships with the stakeholders and is sensitive to understanding each stakeholder's perspective of the issues, priorities, and constraints that drive the engineering effort, including stakeholder expectations and perspective on indicators of success. Examples of roles and responsibilities of possible stakeholders and other individuals associated with the systems security engineering processes can be found in Appendix G.

### *2.1.2 Relationship to Systems Engineering*

The systems engineering discipline executes an interdisciplinary process that delivers a well-specified and well-engineered system to stakeholders.[18] The delivered system meets stakeholder

[16] NIST Special Publication 800-37 describes the *security authorization* process for systems as part of a comprehensive Risk Management Framework integrated into the system life cycle.

[17] NIST Special Publication 800-39 describes the three hierarchical levels (or tiers) where risk management activities occur within organizations.

[18] Systems engineering includes a variety of specialty engineering disciplines and serves as the integrating mechanism for the technical, management, and support activities related to the engineering effort, for example: concept analysis; solution analysis; technology maturation; system design/development; engineering and manufacturing development; production and deployment; training, operations and support; and retirement/disposal.

requirements in a trustworthy, high-quality, cost-efficient, risk-tolerant, and schedule-compliant manner throughout the entire life cycle of the system. Systems security engineering, as an integral part of systems engineering, ensures that the appropriate security principles, concepts, and best practices are applied during the system life cycle to provide the required level of trustworthiness in the delivered system—that is, a level of trustworthiness that the agreed-upon protection needs of stakeholders will be effective on a continuous basis despite disruptions. The systems security engineering discipline provides the security perspective to the systems engineering processes, activities, tasks, products, and artifacts, with emphasis on system security risk management. These processes, activities, and tasks are conducted in consideration of: (i) the technical, physical, and procedural system elements; (ii) the processes employed to acquire system elements and to develop, deliver, and sustain the system; (iii) the behavior of the system in all modes of operation; (iv) the manner in which the system might be attacked or misused; and (v) the security-relevant effects of incidental, accidental, fault, failure, and disaster events.

Systems engineering is a collection of system life cycle processes that encompass technical and nontechnical activities and tasks. The technical processes apply engineering design principles and concepts to deliver a functional system with the capability to satisfy stakeholder requirements; the nontechnical processes apply best practices to manage agreements, provide engineering project management, and facilitate project-enabling support by the engineering organization. Systems security engineering processes, activities, and tasks represent a subset of the parent systems engineering processes, activities, and tasks. Systems security engineering processes provide security-focused contributions that supplement or extend the systems engineering activities and tasks. Chapter Three provides a detailed description of the particular systems security engineering contributions to the systems engineering processes in ISO/IEC/IEEE 15288.

## 2.2 SYSTEM AND SYSTEM ELEMENTS

This section initially discusses the concepts of *system* and *system-of-interest* as used within the engineering community and subsequently describes those terms from the security perspective and the perspective of systems security engineering.

### *2.2.1 System*

A system is a combination of interacting elements organized to achieve one or more stated purposes. Each element of the system (i.e., system element) is implemented to fulfill specified requirements. A system element can be a discrete component, product, service, subsystem, system, infrastructure, or enterprise. The recursive nature of the term *system element* allows the term *system* to apply equally when referring to a discrete component or to a large, complex, geographically distributed system-of-systems. System elements are implemented: (i) by hardware, software, and firmware that perform operations on data/information; (ii) by physical structures, devices, and components in the environment of operation; and (iii) by the people, processes, and procedures for operating, sustaining, and supporting the system elements. Individual or combinations of system elements may satisfy system requirements. Interconnections between system elements allow the elements to interact as necessary to fulfill the system requirements. Finally, every system operates within an environment that has influence on the system and its operation.

Because the term *system* applies equally to any system element or any combination of system elements, the context within which the term *system* is being used must be communicated and understood. Distinguishing context is important because one observer's system may be another observer's system element. The term *system-of-interest* is used to define the set of system

elements, system element interconnections, and the environment that is the particular focus of the engineering effort. The focus of the engineering effort is typically determined by programmatic, operational, or jurisdictional authority and control responsibility. Refinement of the engineering focus may be determined by a decomposition of the system based on architectural, geographic, or some other boundary decision that helps to manage the size and complexity of the system.

The term system-of-interest establishes the *context* for all of these cases. The engineering effort focuses on its particular system-of-interest and the system elements that contribute to satisfying the stakeholder requirements that are not part of the system-of-interest. System elements that are not part of the system-of-interest may place constraints on the system-of-interest and, therefore, on the engineering of the system-of-interest. The engineering of the system-of-interest attempts to comply with all constraints imposed by those system elements unless the constraints are formally removed. The engineering effort must be cognizant of the various views of the system and all its elements despite placing focus on the view that is the system-of-interest. Figure 2 illustrates the systems engineering view of the system-of-interest.

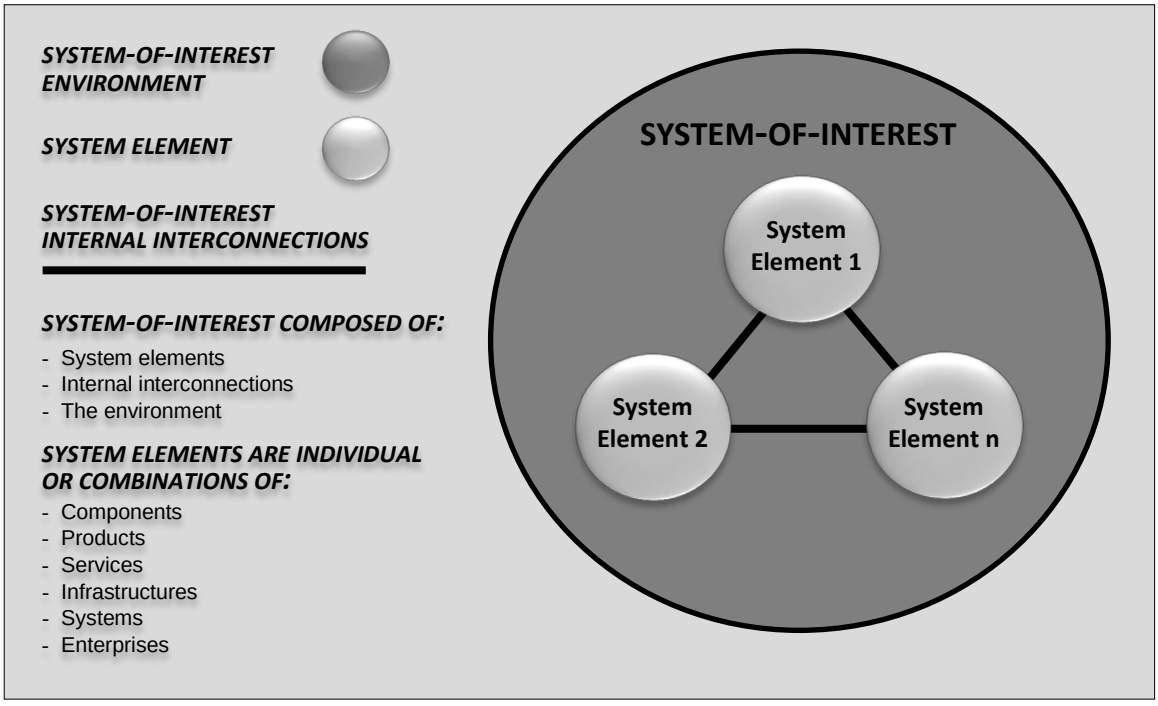


**FIGURE 2: SYSTEMS ENGINEERING VIEW OF THE SYSTEM-OF-INTEREST**

The characteristics of systems vary and can include for example: (i) criticality/importance; (ii) sensitivity of data/information processed, stored, or transmitted; (iii) consequence of loss, failure, or degradation; and (iv) monetary or other value. The characteristics of systems range from those systems for which the consequences of degradation, loss, or erroneous function are insignificant, to systems where the consequences of degradation, loss, or erroneous function have significant monetary, life-threatening, reputation, or other unacceptable consequences. Examples include: (i) general/special-purpose information systems; (ii) cyber physical systems; (iii) command, control, and communication systems; (iv) industrial/process control systems, cryptographic modules, and processor boards; (v) flight and transportation control systems; (vi) weapons, targeting, and fire control systems; (vii) medical device and treatment systems; (viii) merchandising transaction, financial, and banking systems; and (ix) social networking and entertainment systems.

Systems are man-made to deliver a specified capability. The capability may be delivered as services, functions, operations, or a combination thereof. The services, functions, and operations may: (i) directly or indirectly interact with, control, or monitor physical, mechanical, hydraulic, or pneumatic devices, other systems or capabilities; or (ii) provide the ability to create, manipulate, access, transmit, store, and share data and information. Regardless of the type of system or the composition of the system, the reliance on hardware, firmware, and software means that system-level data flows and control flows are what enable the system to function and to deliver the protections required by the mission/business. Therefore, the system must possess designed-in capability for self-protection (including internal data, functions, and mechanisms of the system) in order to deliver the protection capability required by stakeholders.

### *2.2.2 Security View of a System*

The security view of the system focuses on the protection capability that is engineered and the security quality property that is achieved. The engineered protection capability is delivered as an integral part of the system capability. This capability satisfies the stakeholder protection needs in the same manner that the functional capability satisfies the stakeholder mission/business needs. The quality property of security is represented by attributes associated with the behavior of the system when configured and used to enforce a mission/business-driven security policy based on the concept of operations for the system or solution. All systems security engineering processes, activities, and tasks contribute to the achievement of the resultant security quality property.

The protection capability that is realized at the system level is composed of multiple cooperating point-protections and end-to-end protection capabilities.[19] These individual protections may result from dedicated and/or shared protection mechanisms. The system is decomposed into security-specific architectural views and interpretations to better understand and manage the complexity associated with the engineering and assuring of the protection capability. The decomposition of the system is based on *security relevance*, *trust*, and *trust relationships*. Security relevance makes it possible to distinguish those system elements that satisfy protection needs from the other parts of the system. The security architecture[20] demonstrates: (i) how security-relevant mechanisms are allocated to system elements (making those elements trusted system elements); (ii) the trust relationships between the trusted system elements; (iii) the interconnections and information flows that realize the trust relationships; and (iv) how the trusted system elements combine and interact with each other and with the other parts of the system to deliver the specified protection capability. The security architecture provides the basis for understanding the different levels of trust within the system, where the levels of trust exist, the information flows that occur within a level of trust, and the information flows that cross trust level boundaries. This understanding informs the allocation of functional and assurance requirements to security-relevant system elements and provides the basis for trade decisions and security risk management.

With a high-level security architectural understanding in place, focus is subsequently directed at the internals of the security-relevant system elements, applying these same security-relevant, trust, and trust relationship concepts in smaller contexts to successively decompose the system into its primitive components. This iterative decomposition and understanding of the system

[19] An example of a point-protection mechanism is a firewall that controls the information flow between two networks. An example of an end-to-end protection is a virtual private network (VPN) trusted channel between two end-points.

[20] The *security architecture* is a set of physical and logical security-relevant representations (i.e., views) of system architecture that conveys information about how the system is partitioned into security domains and makes use of security-relevant elements to enforce security policies within and between security domains based on how data and information must be protected.

builds confidence through the accumulation of evidence about the internals of individual system elements, how the elements combine to form composite system elements, and how the composite system elements combine to form the system.

Individual protection capabilities may be linked to: (i) mission/business processes; (ii) system functions and processes that exist for the system to operate securely and for its self-protection; or (iii) for system security management functions. The systems security engineering challenge is to preserve the appropriate scope and focus—whether the required protections are being engineered for the new system that emerges from a concept or for the system that requires composing a capability from existing capabilities that are provided by existing systems and infrastructures. Figure 3 illustrates the systems security engineering view of the system-of-interest.

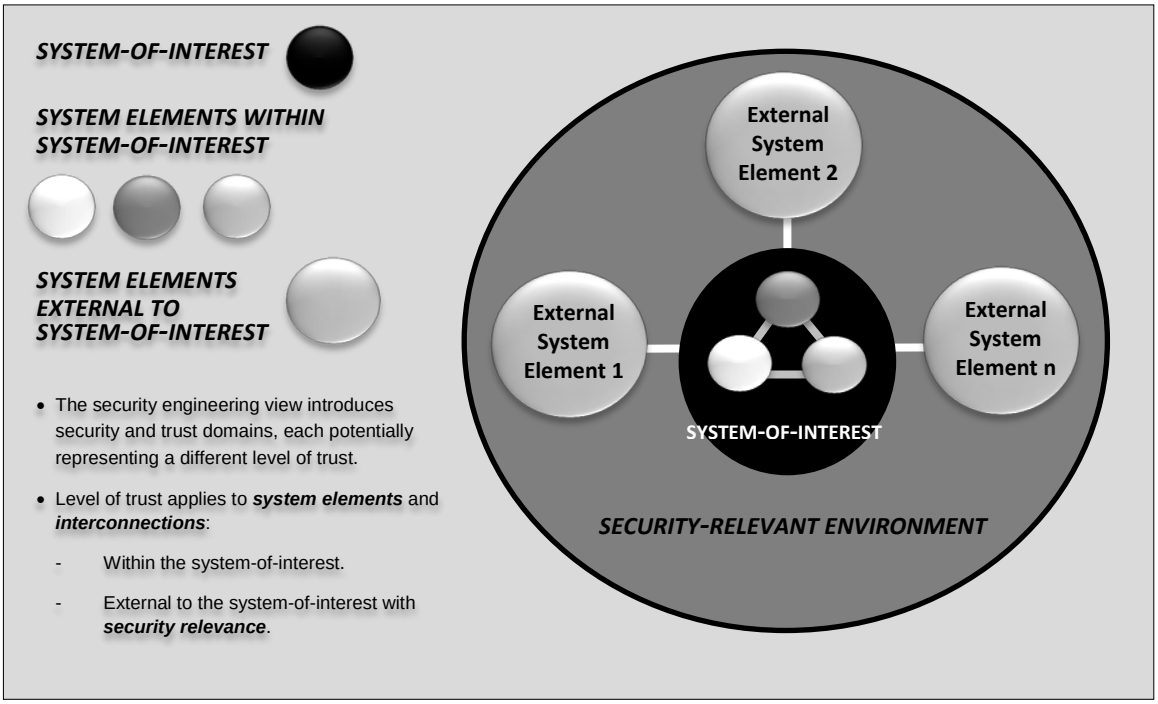


**FIGURE 3: SYSTEMS SECURITY ENGINEERING VIEW OF THE SYSTEM-OF-INTEREST**

## 2.3 SYSTEMS SECURITY ENGINEERING CONCEPTS

This section discusses the foundational systems security engineering concepts that establish the basis for understanding what needs to be protected, for engineering the specified protections such that they provide a trustworthy security protection capability, and for managing the security risk associated with implemented protections. These systems security engineering concepts include: (i) protection needs; (ii) security relevance; (iii) trustworthiness and assurance; and (v) security risk management.[21]

[21] Appendices E and H provide additional detailed discussion and explanation regarding the fundamentals of security, trustworthiness, assurance, and risk management.

### 2.3.1 Protection Needs

Protection needs are defined for all organizational assets and are determined by the potential adverse *impact* of loss. These needs are expressed as the confidentiality, integrity, and availability protections deemed necessary and sufficient to protect stakeholder and system assets. Having established an understanding of the need for protection, the protection needs are then satisfied by the employment of *protective measures* (i.e., security mechanisms, physical mechanisms, and processes/procedures performed by individuals) that are deemed adequate to protect the assets. The selection of protective measures is informed by the *threats* that are anticipated across all system life cycle stages.

Understanding the scope of protection needs is a foundational systems security engineering responsibility. Protection needs are determined from an analysis of multiple inputs from: (i) the *stakeholder* perspective (e.g., mission/business needs, concepts of operations and sustainment, mandates expressed by laws, regulations, and governing organizational policy, organizational constraints); (ii) the *system* perspective (e.g., system architectural design and implementation decisions, system self-protection capability, secure system management functions); and (iii) *trades* perspective (e.g., requirements trades, engineering trades, risk treatment trades). Figure 4 illustrates the key input sources used to define protection needs from all three perspectives and the outputs derived from the specification of those needs.

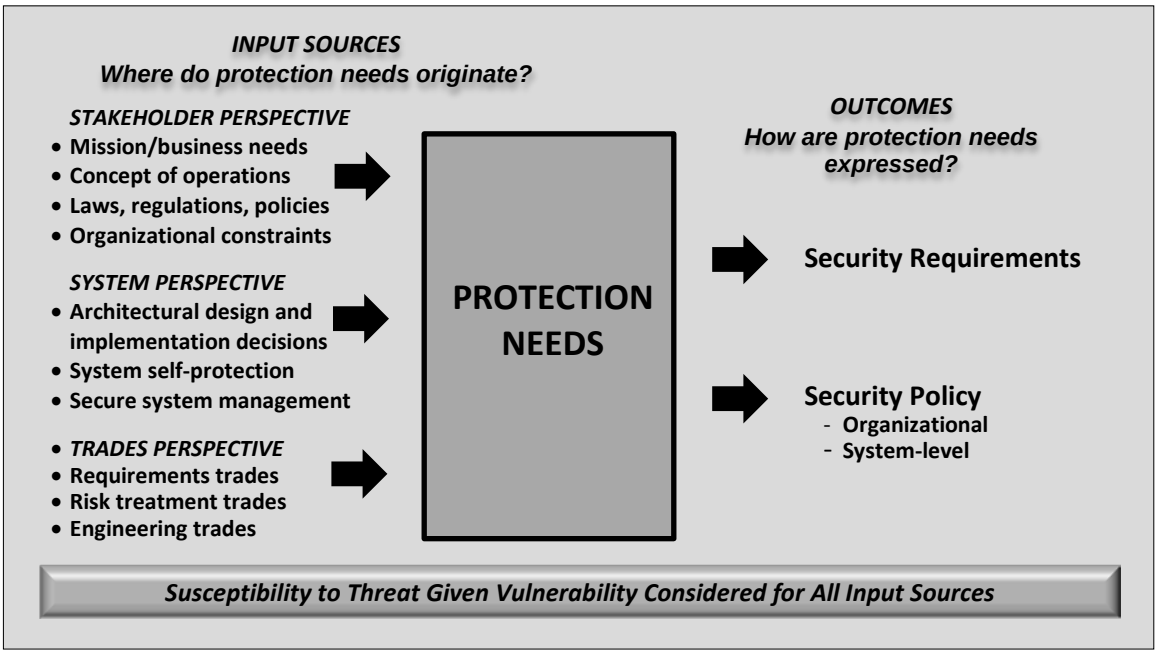


**FIGURE 4: DEFINING PROTECTION NEEDS**

Stakeholder protection needs are formalized and expressed as *security requirements* and in various abstractions of security policy at the organizational and system levels.[22] The periodic revisiting of the stakeholder protection needs contributes to the completeness of the protection capability for the system and its effectiveness in enabling the secure operation and sustainment of the system.

[22] Security requirements determine the protection capability for a system. Security policy determines how the selected protections are to be used.

### 2.3.2 Security Relevance

Security relevance is the term used to describe those functions/mechanisms that directly or indirectly provide the capability to enforce security policy.[23] The concept of security relevance forms a continuum that represents the relationship between a function/mechanism and its significance (i.e., role, importance, and impact) in the enforcement of security policy. This continuum, in order of greatest to least significance, can be expressed as the following types:[24]

- Security-enforcing functions. Security-enforcing functions are directly responsible for making or enforcing security policy decisions.[25] An example of a security-enforcing function is one that makes the decision to grant or deny access to a resource.
- Security-supporting functions. Security-supporting functions contribute to the ability of security-enforcing functions to make or enforce security policy decisions. These functions provide data, services, or perform operations upon which security-enforcing functions are dependent. Validating public key infrastructure (PKI) certificates used to make the decision to grant or deny access to a resource is an example of a security-supporting function.
- Security non-interfering functions. Security non-interfering functions do not enforce or support any aspect of security policy. However, these functions are security-relevant because they have the potential to adversely affect (i.e., interfere with) the correct operation of security-enforcing and security-supporting functions. This condition results from architectural design trade decisions that are driven by other capability needs or by constraints that cannot be ignored.[26] Therefore, the functions designated as security non-interfering cannot be assumed to be so and they cannot be ignored. The functions are assessed and understood within the context of the architectural design for the system such that it is possible to: (i) verify the functions are non-interfering; or (ii) determine the extent to which the functions can interfere with security-enforcing/security-supporting functions so that the risk may be addressed.

Security-relevant functions contribute to satisfying the security requirements. Therefore, the functions must be verified and validated for correct operation, for their ability to behave in a predictable and mutually supportive manner, and for their ability to enforce security policy. The purpose for distinguishing among the types of security relevance is to ensure that the appropriate types of analysis are performed to accurately determine the scope of the security system. The fact that one part of the system is security-enforcing while another is security-supporting does not automatically dictate the need for or allow acceptance of more or less assurance, trustworthiness, or risk tolerance. Instead, security-enforcing and security-supporting functions/mechanisms and any relevant security non-interfering functions/mechanisms must be assessed in terms of how they compose and interact to provide protection capability. Those assessments inform decisions

[23] In addition to the functions and mechanisms that enforce security policy from hardware, firmware, and software, personnel also perform functions that contribute to security policy enforcement.

[24] International Standard ISO/IEC 15408 refers to functions/mechanisms as security functional requirement (SFR) enforcing, SFR supporting, or SFR non-interfering. This naming convention allows differentiation of the degree to which a function/mechanism satisfies a security requirement. The discussion in this document abstracts the concept in ISO/IEC 15408 to the level of security policy enforcement while preserving the same intent as in the standard.

[25] Defining the scope of a security policy and determining the rules that compose the security policy is a necessary first step to the enforcement of the policy.

[26] For example, to satisfy a size or form-factor constraint may require a security non-interfering function to share resources (e.g., memory, CPU) with security-enforcing or security-supporting functions. If that constraint did not exist, it would be prudent to avoid such sharing—adding to the assurance that the security-enforcing/supporting functions are better isolated from other parts of the system and will not be adversely impacted by their behavior or provide an avenue for attack.

for how best to ensure that security-relevant functions/mechanisms have the necessary assurance, trustworthiness, and risk deemed acceptable to stakeholders. Systems security engineering also brings the ability to accurately determine security relevance to the engineering effort. To do so, systems security engineering activities must be accomplished as part of all systems engineering tasks to ensure that the security-relevant portions of the system are properly identified. Only then can all security-relevant issues be adequately addressed by the systems engineering effort.

### Security Policy

System security is a condition[27] that results from the establishment and sustainment of protective measures that contribute to continuous achievement of mission/business objectives despite risks posed by potential threats throughout the system life cycle.[28] The condition that determines what it means for a system to be secure is specified by *security policy*. Security policy is a fundamental computer security concept that differs from security requirements.[29] Security policy is a set of rules that governs all aspects of security-relevant behavior of individuals and processes acting on behalf of individuals. Such security-relevant behavior can be exhibited, for example, by systems, subsystems, components, mechanisms, services, and infrastructures.[30]

Security policy is enforced: (i) by individuals (i.e., procedurally); (ii) by devices in the physical environment (i.e., physically); and (iii) by automated mechanisms implemented in the hardware, firmware, and software of the system. Security policy is intended to be enforced continuously[31] and is intrinsically related to the concepts of trust and trustworthiness. One condition that must be satisfied for a system to be deemed trustworthy is that there is sufficient confidence or assurance that the system is capable of enforcing security policy on a continuous basis. The implications associated with demonstrating the continuous enforcement of security policy at the system level is what distinguishes systems security engineering from its composite security specialties and from systems engineering and related engineering specialties—particularly those concerned with accuracy, availability, fault tolerance, performance, reliability, sustainability, human safety, and general functional correctness. Security policy is expressed in terms of the foundational security properties of *confidentiality*, *integrity*, and *availability*.

- Confidentiality. Rules that govern access to, use of (i.e., operations that can be performed on), and disclosure of resources. While confidentiality policy typically applies to information and data, it may also apply to protect the knowledge of and the use of capabilities operating on the data (e.g., functions, mechanisms, services, and infrastructures);
- Integrity. Rules that govern the authorized manners in which data, information, and other resources (e.g., mechanisms, functions, processes, services, and infrastructures) can be manipulated; and

[27] Webster's dictionary defines security as a quality, state, or condition of being secure.

[28] This definition, adapted from CNSS Instruction 4009, reflects an *organizational enterprise* perspective and captures the total-system perspective of systems engineering and systems security engineering.

[29] Appendix H explains the difference between *security policy* and *security requirements* in the discussion regarding the fundamentals of security and trustworthiness.

[30] Computer processes may execute on behalf of an individual. A protected binding is used to associate the security-relevant attributes of an individual with a process that executes on behalf of the individual. The binding makes it possible to restrict the behavior of the process such that it can perform only those operations that the individual is authorized to perform.

[31] Appendix H explains the concept of *continuous protection*, one of the principles of trusted systems development.

- Availability. Rules that govern the ability to access and use data, information, or a resource.[32]

Security policy addresses all aspects of confidentiality but only the security-relevant aspects of integrity and availability. Whereas *confidentiality protections* against unauthorized access and unauthorized disclosure of resources are fully addressed by the security discipline, the scope of *integrity protections* and *availability protections* are addressed by the combination of security and other specialty disciplines.[33] The integrity and availability scope overlap leads to confusion when the basis for the protection need is not properly allocated or understood. The confusion is often the source of design conflicts and contradictions that are best resolved through informed trade space analysis among all impacted and contributing disciplines. Security policy distinguishes the security-relevant aspects of integrity protections and availability protections from the integrity and availability protections that are addressed by other specialty disciplines. Figure 5 illustrates the scope of security policy properties.

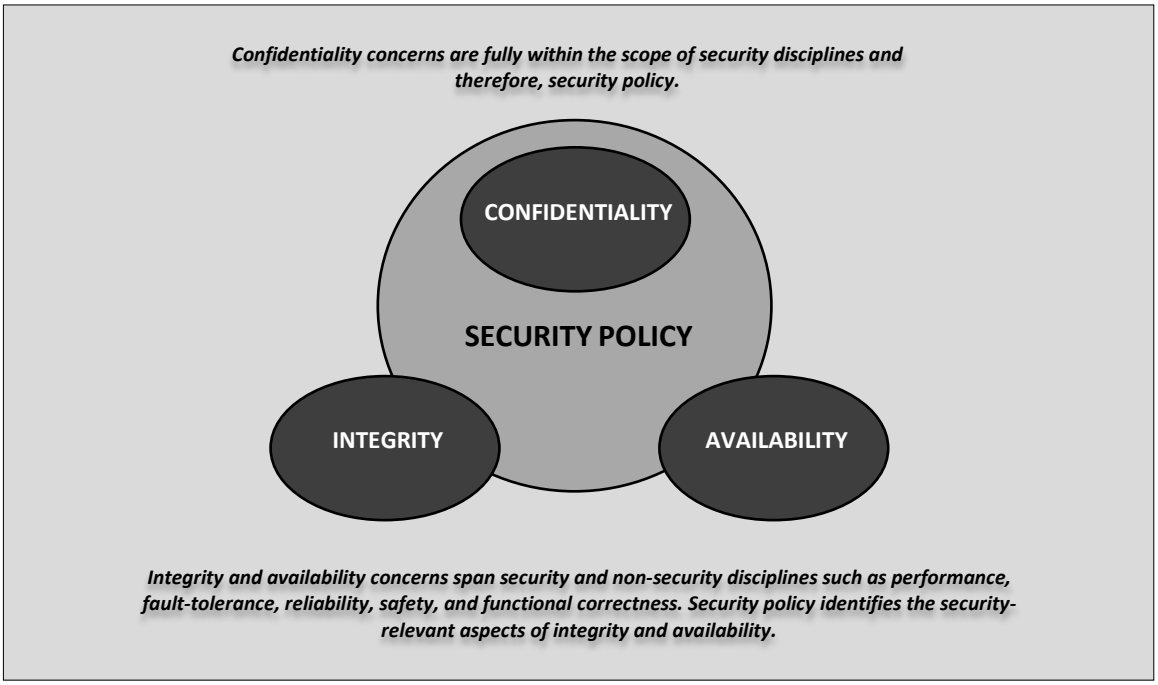


**FIGURE 5: SECURITY POLICY PROPERTIES SCOPE**

The term *security policy* is used in several ways, including: (i) security policy objectives; (ii) organizational security policy; and (iii) system security policy. There is a hierarchical relationship established among the uses of the term security policy (i.e., security policy objectives subsume

[32] The "ability to access" requires elaboration to differentiate it from its use with respect to confidentiality. The "ability to access" typically means that the data, information, or resource is usable when needed (i.e., able to be used at a point in time). However, the ability to access may be extended to include the case that the data, information, or resource will be continuously usable until no longer required. The "ability to access" should not be confused with "authorization to access" (based on confidentiality).

[33] The capability of a software algorithm to perform calculations with sufficient accuracy and precision, and produce correct results in a delivered capability is not a *security integrity* issue. The capability of a device to continue to operate despite non-catastrophic faults is not a *security availability* issue. However, in each of the above situations, if the loss of integrity or availability results in a violation of a security policy, then there are security-relevant concerns associated with those capabilities.

organizational security policy which in turn, subsumes system security policy). Figure 6 shows the hierarchical relationship among the different uses of the term security policy.

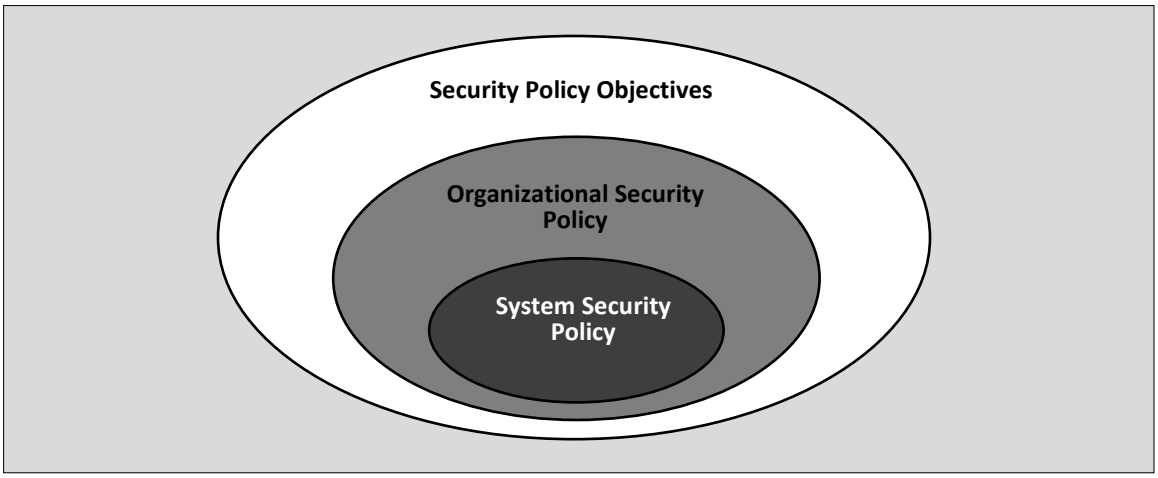


**FIGURE 6: SECURITY POLICY HIERARCHY**

Each use of the term security policy has a different context, authority, scope, and purpose as described below:

- Security Policy (Protection) Objectives. Security policy objectives include a statement of intent to protect identified assets within the specific scope of stakeholder responsibility and security risk concerns. The objectives identify the assets protected and the scope of protection (i.e., specifics of the protections to be provided). Security policy objectives are the basis for the derivation of all other security policy forms.
- Organizational Security Policy. Organizational security policy is the set of laws, rules, and practices that regulate how an organization manages, protects, and distributes assets to achieve specified security policy (protection) objectives. These laws, rules, and practices identify criteria for according individuals authority, and may specify conditions under which individuals are permitted to exercise or delegate their authority. To be meaningful, these laws, rules, and practices provide individuals with a reasonable ability to determine whether their actions violate or comply with the security policy. The laws, rules, and practices that constitute an organizational security policy are highly dependent on the security policy objectives and the organization's analysis of life cycle threats. Organizational security policy defines the behavior of employees in performing their missions/business functions and is used for development of processes and procedures.
- System Security Policy. System security policy (i.e., automated security policy) specifies what a trusted system is trusted to do. It is the set of restrictions and properties that specify how a system enforces or contributes to the enforcement of an organizational security policy.[34] This includes, for example, defining how an operating system governs executing processes and the use of system resources, or how a firewall mediates the flow of incoming and outgoing data packets. The system security policy has the restriction that its scope of authority is limited to

[34] System security policy may be reflected in semiformal or formal models and specifications. Mathematical methods and techniques (e.g., formal methods) may be used to provide assurance in the correctness of security policy models. The models and specifications are used as the basis for design and implementation of the mechanisms that enforce the policy. Verification activities demonstrate that the mechanism is a correct implementation of the security policy model.

the resources within the scope of control of the system. Each instance of a system security policy is properly matched to the set of resources that are within the scope of control of the system and the capabilities of the security-relevant elements of the system that enforce the system security policy. Any resource operation that is not authorized by or specified by the system security policy violates organizational security policy. The transformation of an organizational security policy to a system security policy is supported by policy-driven verification and validation activities that are equivalent to those used to verify the system against its design requirements and to validate the system against stakeholder requirements.[35]

From the systems security engineering perspective, security policy objectives and all subsequent security policy forms are derived from *protection needs*. Protection needs are identified from a variety of inputs provided by stakeholders. These stakeholder inputs are assessed and transformed into the security requirements that specify the security capability needs that are to be satisfied. As part of security architectural design activities, security policy objectives are allocated to physical, personnel, and automated protective measures. This is accomplished in parallel with security requirements allocation and the subsequent decomposition of requirements as the design matures. That is, security policy goes through an iterative refinement that decomposes a more abstract statement of security policy into more specific statements of security policy. The objective is for the decomposition of security policy to be matched to the capabilities of the security-relevant elements that are allocated the responsibility for security policy enforcement. Figure 7 illustrates the allocation of security policy enforcement responsibilities.

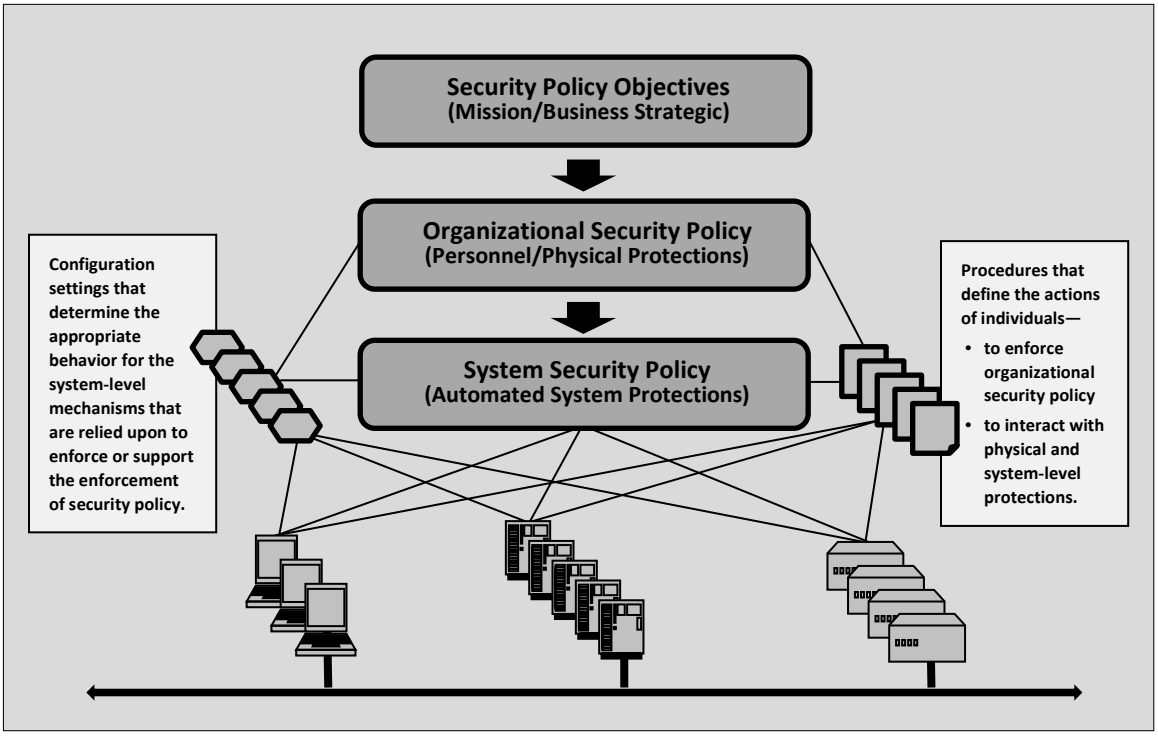


**FIGURE 7: ALLOCATION OF SECURITY POLICY ENFORCEMENT RESPONSIBILITIES**

[35] System security policy and security requirements differ. A security requirement specifies functional, assurance, and strength characteristics for a protection mechanism (e.g., the capability for an access control function to mediate access to objects based on classification and access mode). The related security policy specifies the necessary behavior of that protection mechanism to support mission/business operations (e.g., the grant/deny rules for a specific list of individuals and their authorization to perform operations on a specific list of objects).

Protection needs are transformed into expressions of security policy appropriate to the level within the hierarchy that has responsibility for enforcement. At the organizational security policy level and below, each expression of security policy includes a related set of processes and procedures.[36] The various expressions of security policy combine to establish the conditions within which the system is considered to be secure. Therefore, any discussion or activity that involves a security policy must be able to: (i) distinguish the parts of security policy that govern human behavior from the parts of security policy that govern physical and system-level mechanisms; (ii) demonstrate consistency, dependency, and traceability between all parts of security policy; and (iii) demonstrate that the combination of all security policy forms together satisfy the security policy objectives and protection needs of stakeholders.

### *2.3.3 Trustworthiness and Assurance*

Systems security engineering delivers measurable protections that are capable of operating as intended despite errors, faults, disaster events, and purposeful attacks. The trustworthiness of the system is not achieved simply by composing individually trusted component parts. Rather, in order for stakeholders to deem a system as being sufficiently trustworthy for its intended use, there must be sufficient confidence/assurance that the protections: (i) are properly implemented and integrated; (ii) can be relied upon to enforce the security policy; (iii) achieve the desired outcomes; and (iv) achieve such outcomes without presenting unacceptable risk. The three concepts of *trust*, *trustworthiness*, and *assurance* are fundamental to achieving these objectives.[37] These concepts are closely related to each other and inform security risk management. They also share the same need for credible and relevant evidence which, when subjected to analysis and scrutiny, is deemed sufficient to substantiate that the system is trustworthy, warrants the trust that is to be placed on it, and presents residual risk that is acceptable and manageable to stakeholders.

Trust, in general, is the *belief* that an entity will behave in a predictable manner while performing specific functions in specific environments and under specified conditions or circumstances.[38] The entity may be a person, process, system element, system, system-of-systems, or combination of these entities. Trust, from the security perspective, is the belief that a security-relevant entity will behave *only* in a predictable manner when satisfying protection needs under specified conditions or circumstances and while subjected to disruptions, component faults and failures, human errors, and purposeful attacks that may occur in the environment of operation. Trust may be determined relative to a specific protection need capability provided by an individual system element or the entire system. However, trust at the system level cannot be achieved by simply interconnecting a set of trusted system elements to compose a system-wide protection capability. Rather, trust at the system level is derived from assurance; acquiring an understanding that builds confidence in the behavior and interactions among system elements (i.e., individuals, technical components, and physical components), taking into account the life cycle activities that govern, develop, operate, and sustain those elements. In essence, the decision to trust a system protection capability requires a sufficient body of evidence upon which the trust decision can be made.

The concept of trustworthiness follows from the concept of trust. Trustworthiness, in general, is an *attribute* associated with an entity that reflects confidence that an entity is *worthy of the trust*

[36] These processes and procedures address items such as device installation, calibration, configuration, maintenance, and proper use.

[37] Systems security engineering focuses on trust, trustworthiness, and assurance relative to the mechanisms, processes, services, policies, and systems that compose the security elements of a system.

[38] The specified conditions or circumstances include those that define the manner in which separate entities are expected to behave while interacting for the exchange of data and information, or in providing capability or services.

required by some other entity. Trustworthiness, from the security perspective, is an attribute that reflects confidence that a security-relevant entity warrants the trust that is be placed on it relative to how that entity provides or contributes to a protection capability. Trust and trustworthiness are related in that the level of trust that should be placed in an entity is related to the trustworthiness that has been established in that entity—a more trustworthy entity warrants placement of greater trust than a less trustworthy entity. And in a similar manner, the trustworthiness of an entity is best substantiated by having established confidence or assurance about the entity. Assurance is obtained from reasoning about evidence that is associated with the entity. The trustworthiness of a protection capability may be based on multiple dimensions of assurance associated with the elements that compose the protection capability. Figure 8 illustrates the relationship between trustworthiness and assurance.

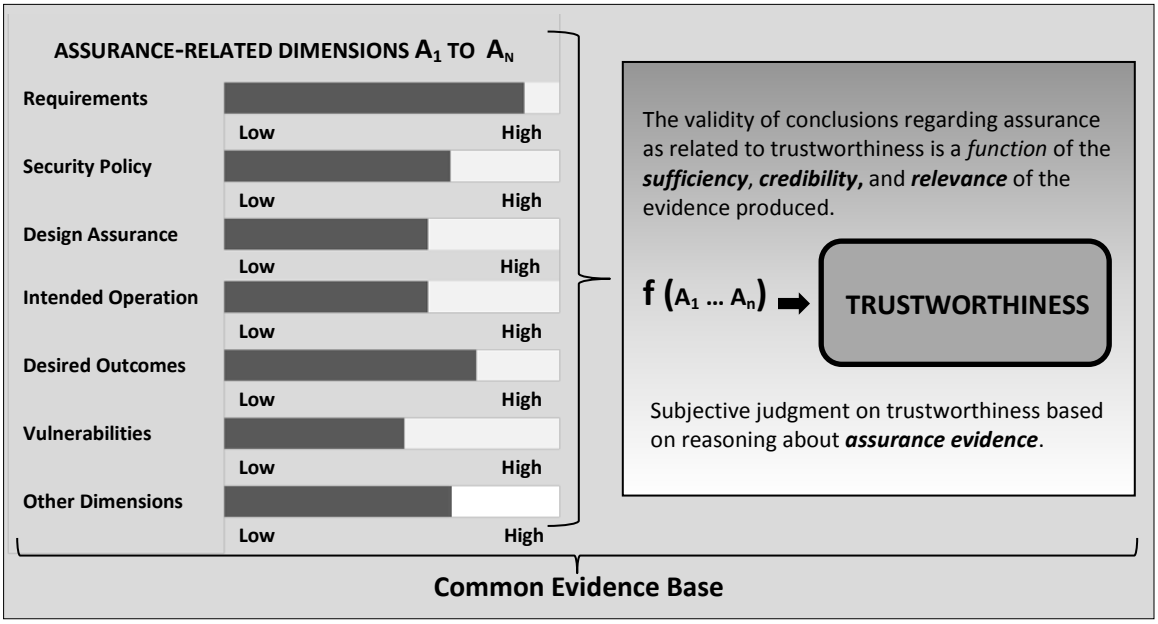


**FIGURE 8: MULTIPLE DIMENSIONS OF ASSURANCE CONTRIBUTING TO TRUSTWORTHINESS**

From the systems security engineering perspective, the trustworthiness of a protection capability is a function of how the trustworthiness of the elements that compose the protection capability is leveraged. Trustworthiness does not just happen—it is a by-product of a purposeful architectural design and implementation supported by adherence to foundational security principles, and achieved by rigor in the application of developmental processes.[39] The trustworthiness of individual system elements is determined by first obtaining evidence that provides assurance about how the individual elements satisfy any claims[40] associated with the protections they each provide. Next, the system elements that compose the protection capability are considered in combination, and additional evidence is obtained to provide assurance about how the composed capability satisfies claims associated with the protections they provide. This iterative building-block approach can be performed using abstractions such as architectural decomposition of the system, mission/business process flows, or end-to-end data, information, or control flows. In each case, the assessment determines the degree of trustworthiness that can be placed on the protection

[39] Trustworthiness principles are discussed in Appendix H.

[40] Claims are statements of something deemed to be true including associated conditions and limitations. The term *claim* should not be equated with assurance case, and claims are not equivalent to requirements.

capability and the acceptability of that degree of trustworthiness.[41] This assessment is conducted in a configuration that results in protection behavior appropriate to support the mission/business operations.

Security functional requirements, security assurance requirements, and security policy combine as the means that establish the basis for trustworthiness. Security functional requirements specify the capability of protective measures (i.e., what the measures must be able to do) and the behavior of the protective measures (i.e., how the measures operate). Security policy specifies what is and is not allowed relative to organizational security policy objectives (i.e., how the protective measures must *actually behave* in the specific operational context). Security assurance requirements state the assurance evidence necessary to verify/validate that: (i) the security functional requirements are satisfied; and (ii) the security policy is properly enforced. Security assurance requirements also specify the verification and validation activities to be performed to generate, analyze, and interpret the assurance evidence.

Assurance, in a general sense, is the *measure* of confidence that an entity meets its requirements. From a security perspective, assurance is the measure of confidence that the protective measures: (i) satisfy protection needs specified by the stakeholders; (ii) satisfy design security requirements; (iii) behave only as specified by those requirements; (iv) enforce security policy; (v) mitigate vulnerabilities;[42] (vi) achieve the desired outcomes; and (vii) are effective in reducing risk. Assurance is obtained as a result of verification and validation activities that generate credible and relevant evidence[43] to substantiate claims made about the security capabilities, properties, vulnerabilities, and the effectiveness of protective measures in satisfying protection needs. These activities target the combination of technical, physical, and human system elements, to include the system life cycle processes and procedures associated with those system elements. Security assurance-focused verification and validation activities are incorporated into each of the systems security engineering technical processes to build a security body of evidence. The accumulation of security evidence traced to outcomes of the engineering processes is what builds assurance in the protective measures.

Assurance evidence serves as the foundation for substantiating the trustworthiness and risk associated with protective measures and system level protection capability. The evidence to be generated is therefore tied to trustworthiness and risk goals. An analysis of trustworthiness and risk goals allows derivation of specific claims about the protections. Security assurance requirements then specify the evidence to be obtained and the verification and validation techniques and methods employed to acquire or generate the evidence.

[41] The decision to trust the system for operational use includes the decision to accept residual risks.

[42] Not all vulnerabilities can be mitigated to an acceptable level. There are potentially three classes of vulnerabilities in delivered systems: (i) vulnerabilities whose existence is known and either eliminated or made to be inconsequential; (ii) vulnerabilities whose existence is known but that are not sufficiently mitigated; and (iii) unknown vulnerabilities that constitute an element of uncertainty—that is, the fact that the vulnerability has not been identified should not increase confidence that the vulnerability does not exist. Identifying the delivered residual vulnerabilities and the risk posed by those vulnerabilities, and having some sense of the uncertainly associated with the existence of the unknown residual vulnerabilities is an important aspect of assurance.

[43] Assurance evidence may be objective or subjective. Some security evidence can support arguments of strength of function, negative requirements (i.e., what will not happen), and qualitative properties. Subjective evidence is analyzed in the intended context and correlated to the claims it supports via rationale. There is not a direct correlation between the type of evidence or the quantity of evidence and the amount of assurance that is derived from the evidence.

The evidence used to substantiate claims can be objective or subjective.[44] Evidence may be obtained directly through measurement, testing, observation, and inspection, or indirectly through the analysis of data obtained from measurement, testing, observation, or inspection. Due to the subjectivity associated with some forms of evidence, the interpretation of evidence and resultant findings may also be subjective.

***Illustrating the Difference Between Trustworthiness and Assurance***

Consider the process of issuing a security clearance. An investigator conducts a full background check on an individual and collects evidence in many dimensions. This *assurance* evidence is presented to the adjudication committee to determine if such evidence constitutes a sufficient basis to *trust* the person with handling sensitive information. The evidence can be compelling in favor of granting the clearance or in favor of denying the clearance. Alternatively, the evidence may be inconclusive and require a subjective decision to grant or deny the clearance.

Claims reflect the desired attributes of protections and are best derived from risk concerns such as: (i) how well protections are implemented; (ii) the degree to which protections are susceptible to vulnerabilities and contain latent errors; (iii) the ability of protections to exhibit predictable behavior while operating in secure states;[45] and (iv) the ability of protections to resist, respond to, or recover from specific attacks. Claims can be expressed in terms of: (i) functional correctness;[46] (ii) strength of function; (iii) specific confidentiality, integrity, or availability concerns; and (iv) the protection capability derived from the adherence to standards, and/or from the use of specific processes, procedures, and methods.

Assurance is obtained in three interacting dimensions of *scope*, *depth*, and *rigor*.[47]

- Scope. Assurance is increased by focusing effort on a larger portion of the system and its supporting developmental, field engineering, operations, and sustainment processes;
- Depth. Assurance is increased by the effort expended to a finer level of introspection into the architectural design and implementation of the system and into the finer aspects of supporting and enabling processes; and
- Rigor. Assurance is increased by the effort expended to perform activities and to generate artifacts in more structured, formal, and consistently repeatable manner given the scope and depth within which effort is expended.

The level of assurance obtained in a protection capability can be tailored by adjusting the scope, depth, and rigor of assurance techniques and methods employed to build the evidence base. This

[44] An example of *objective* evidence is pass/fail test results. An example of *subjective* evidence is that which must be analyzed or interpreted, and perhaps combined with other evidence to produce a result.

[45] Secure states include the initial secure state, all subsequent run-time execution states, the halt state, and all transitions between states. Additionally, secure states apply to all specified modes of operation (e.g. normal, degraded, recovery).

[46] Expressing claims solely as security functional and performance requirements or to substitute security functional and performance requirements as claims should be avoided. While this approach does provide assurance that requirements are satisfied, it constitutes an insufficient basis for reasoned decisions of trustworthiness. Such an approach also has the implicit assumption that the security requirements themselves are correct and accurately reflect stakeholder intent.

[47] The three dimensions of assurance are defined in ISO/IEC 15408, *Common Criteria for Information Technology Security Evaluation*.

tailoring strives for optimal cost-benefit trade-offs of assurance-related effort expended and the confidence gained as a result of that expenditure. Assurance trade-off considerations influence the determination of feasibility or appropriateness of one protective measure over another. Assurance cost/benefit trade-off considerations are an integral part of security risk management decisions for the selection of protective measures.[48]

### *2.3.4 Security Risk Management*

*Risk* is a measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence. Risk management is conducted as a holistic, enterprise-wide activity that addresses risk from the strategic level to the tactical level—ensuring that effective risk-based decision making is integrated into every aspect of the system life cycle. Risk is managed within the scope and priority of stakeholder risk concerns. Stakeholder risk concerns are typically associated with: (i) a prioritized set of missions/business functions and associated mission/business processes that are created to help carry out those missions/business functions; (ii) the technology, infrastructure, hardware/software components, and data/information assets used by the organization to enable and support the mission/business processes; and (iii) the capability, performance, and competitive advantage realized by the organization from the sensitive data, intellectual property, capabilities, and systems they rely upon. The response to an identified security risk requires taking any of the following *risk treatment* actions:[49]

- Avoiding Risk. Avoiding risk is accomplished by deciding not to proceed with the activity that generates the risk—in effect, eliminating the likelihood of a specific threat event, eliminating the susceptibility to a vulnerability, or eliminating the consequence or impact. Avoiding risk can include, for example: (i) changing architecture, design, and implementation; (ii) making changes to the concept of operations; (iii) removing requirements; and (iv) avoiding the use of specific technologies, products, or suppliers.
- Accepting Risk. Accepting risk is accomplished by making a conscious decision to pursue an activity despite the risk presented. This includes deciding to expend no effort or to expend no further effort to address the potential for a threat to exploit or trigger a vulnerability or to further reduce the resultant consequence. Accepting risk requires contingency planning that enables the risk to be monitored and responded to in a manner acceptable to the stakeholders impacted by the risk.
- Mitigating Risk. Mitigating risk is accomplished by employing protective measures. These protective measures may: (i) change the consequence or likelihood of a threat exploiting or triggering a vulnerability; or (ii) remove the threat or vulnerability that generates the risk. Risk mitigations do not always eliminate risk. Some residual risk may remain, and that residual risk must be understood, accepted, and managed. Additionally, the employment of protective measures may introduce risk that would not otherwise be present.
- Sharing/Transferring Risk. Sharing or transferring risk is accomplished by allocating all or some of the risk mitigation responsibility or risk consequence to some other organization. Sharing risk requires formal agreements that state the scope, roles, and responsibilities for any risk that the organization shares or transfers.

[48] NIST Special Publication 800-53 provides a comprehensive set of assurance-related security controls to help organizations satisfy security requirements and stakeholder protection needs.

[49] ISO/IEC 31000, *Risk Management—Principles and Guidelines* describes the concept of *risk treatment*. The term risk treatment is synonymous with the term *risk response* in NIST Special Publication 800-39 which describes five potential responses to identified risks: accepting, avoiding, mitigating, sharing, or transferring risk.

Security risk is one of several types of risk managed by stakeholders.[50] Security risks are those risks that reflect the potential for threats to exploit or trigger vulnerabilities with a resultant loss of confidentiality, integrity, or availability of assets to a degree that results in adverse impact or consequences to the organization. The adverse impact/consequences can affect the ability of the organization to carry out its missions/business functions. Security risk is managed within the systems engineering risk management process and includes: (i) planning for risk management; (ii) managing the risk profile; (iii) analyzing/assessing risks; (iv) treating or responding to risks; (v) monitoring risks; and (vi) evaluating the risk management process.[51] Security risk management consists of an integrated set of security-focused activities that enable cost-effective risk treatment decisions resulting in a risk level that is within the specified stakeholder risk tolerance. Security risk management is performed as part of all systems security engineering activities. The outcomes of security risk management activities inform the risk management processes of stakeholders, which facilitates continuous management of delivered security risk throughout the operational and sustainment stages of the system life cycle. Figure 9 illustrates the components of security risk management.

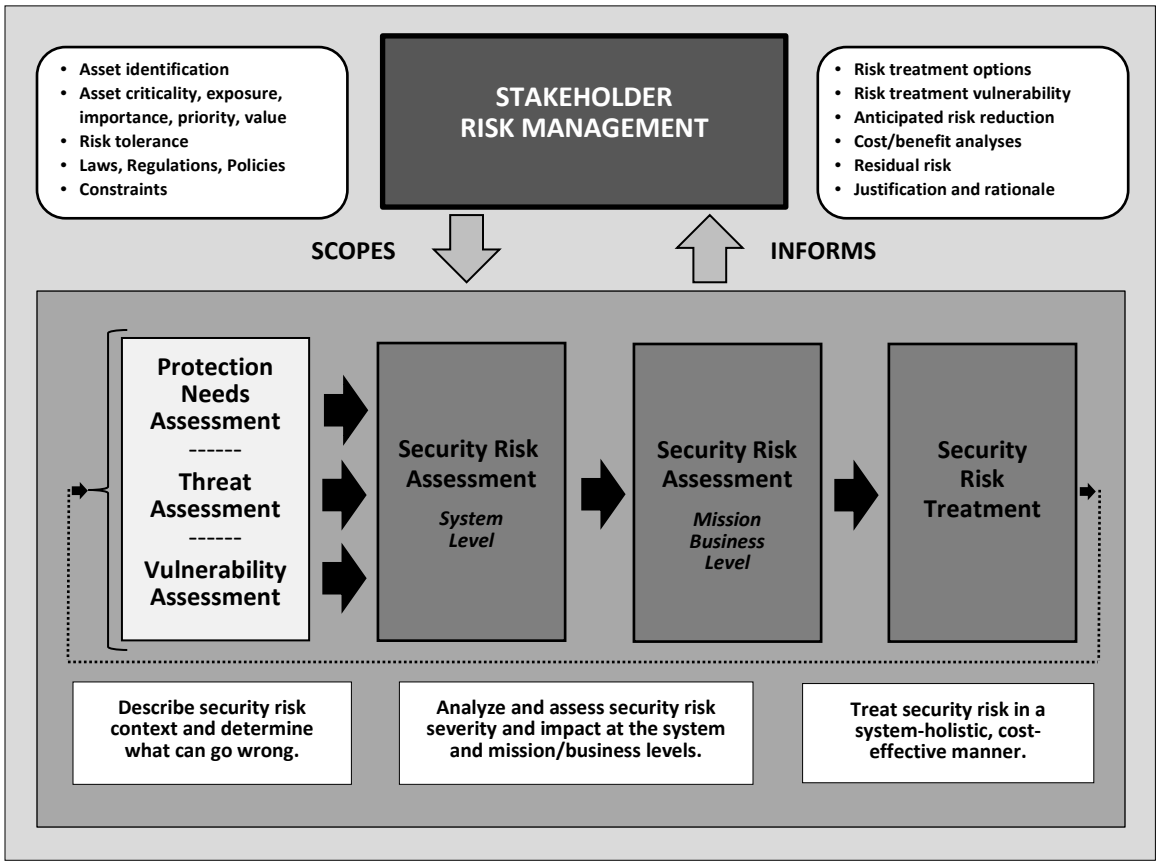


**FIGURE 9: COMPONENTS OF SECURITY RISK MANAGEMENT**

[50] Types of risk include, but are not limited to, mission/business, safety, security, programmatic, monetary, schedule, training, maintenance, and sustainment.

[51] NIST Special Publication 800-39 describes risk management from the organizational, mission/business process, and systems perspective. The publication defines four risk management processes to include: (i) *framing* risk; (ii) *assessing* risk; (iii) *responding to* risk; and (iv) *monitoring* risk.

Security risk management activities determine the following in context of a system description that includes stakeholders, risk management scope and objectives, system intended function, system intended use, system configuration, and the environment of operation:

- The consequences of the loss of confidentiality, integrity, or availability of assets;
- The threats to which the system is subjected;
- The inherent system vulnerabilities;
- The correlation and interaction between the threats and vulnerabilities that can be exploited or triggered;
- The risk (severity and likelihood) of a threat exploiting a vulnerability resulting in the loss of confidentiality, integrity, or availability of an asset;
- The prioritization and ranking of security risk to the system supporting the organization's missions and business functions;
- The selection of security risks for risk treatment (risk response); and
- The identification of feasible risk treatment options and risk treatment/response plans.

Security risk management determines the security-relevant impact at the system level which in turn informs a holistic assessment of impact at the system level, and finally, the assessment of mission/business risk. Security risk management results combine with the results of all other risk management focus areas to provide a comprehensive, organization-wide statement of risk as input to the stakeholder's risk management process.[52] The stakeholders then can execute a balanced risk management strategy to reduce risk to an acceptable level, manage the residual risk, and achieve mission/business capability and trustworthiness objectives across all their risk concerns. Security risk management also requires a broad range of subject matter expertise in a variety of areas within an organization including, for example: (i) the core missions and business functions; (ii) physical, personnel, procedural, and technical security; (iii) systems engineering; and (iv) multi-domain subject matter expertise specific to other critical concerns of stakeholders. Stakeholders representing the operational, sustainment, information owners, and authorization communities have risk decision-making responsibility as they will inherit the risks delivered with the system and are responsible for the management of the delivered risk.

Security risk management activities are executed recursively, perhaps in multiple, concurrent risk contexts and with varying emphasis as part of developmental engineering, field engineering, and operations and sustainment efforts throughout the system life cycle. The activities are repeated with increasing detail and depth: (i) as the system concept and system design matures; (ii) as the protective measures are identified, developed, integrated, and deployed as part of the delivered system; and (iii) as experience with the protective measures grows from use of the system.[53] The risk management activities may also be conducted in support of specific life cycle milestone events and in response to changes associated with mission/business objectives, mission/business processes, concept of operations, threat sources and events, vulnerabilities, and changes in the criticality and categorization of assets.

[52] The Risk Management Framework (RMF) described in NIST SP 800-37 is an example of such a process.

[53] Once a system is delivered, the operational/sustainment community may provide feedback to the engineering team through security problem and incident reports, observations, and findings to inform subsequent developmental efforts. Additionally, field/sustainment engineering efforts may use the same information for problem resolution, upgrades, and enhancements carried out in the operational environment.

### Protection Needs Assessment

A *protection needs assessment* is the method used to identify the confidentiality, integrity, and availability protection needs for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable. As described in Section 2.3.1 and as illustrated in Figure 4, the protection needs assessment is driven by: (i) *stakeholder-related* inputs; (ii) *system-related* inputs; and (iii) *trades-related* inputs. A clear, consistent, and unambiguous understanding of protection need and the resultant impact should those protections be insufficient, nonexistent, or totally ineffective establishes the basis for security risk management.[54]

Initially, the protection needs assessment is driven by the stakeholder's perspective including a determination of: (i) mission/business objectives and processes; (ii) organizational assets (e.g., components, data, functions, information, technology, intellectual property); (iii) asset criticality, exposure, importance, priority, and value;[55] and (iv) environments of operation. The input from stakeholders serves two important risk management needs: (i) it establishes the scope and focus for all security risk management activities; and (ii) it determines the priority for the planning, allocation, sizing, and costing of resource expenditures for the treatment of security risk. The system and trades perspectives become the focal points at subsequent stages in the system life cycle. As the architectural design matures through the verification and validation processes, additional protection needs are identified as a direct result of the design and risk treatment decisions. The scope of the protection needs assessment expands accordingly to include system-level assets and their criticality, exposure, importance, priority, and value relative to the system's ability to function correctly (i.e., securely) and to provide for its own self-protection. Figure 10 illustrates the key components of the protection needs assessment.

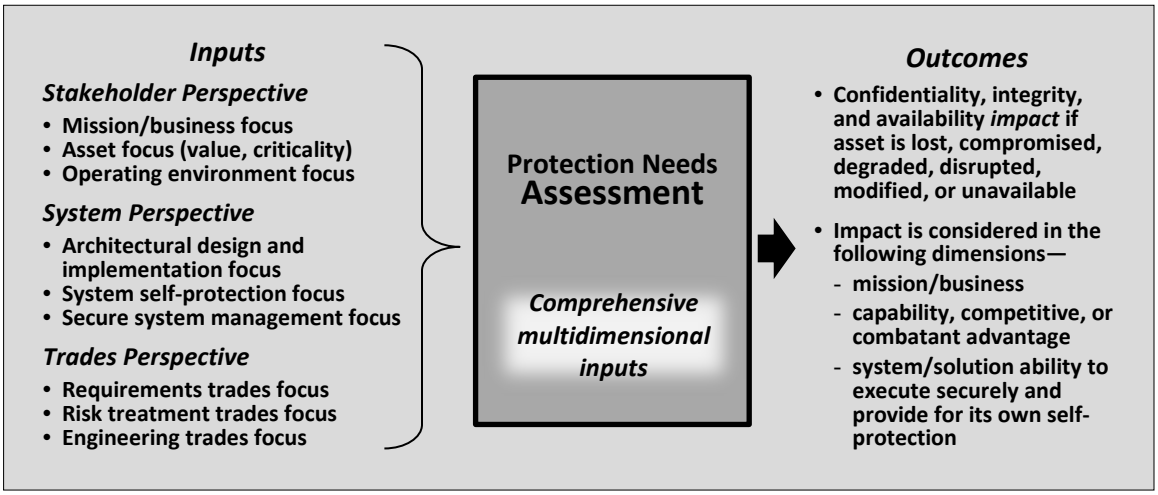


**FIGURE 10: KEY COMPONENTS OF PROTECTION NEEDS ASSESSMENT**

[54] *Protection needs assessment* is also the basis for security requirements elicitation and analysis, the identification of derived requirements associated with architectural design decisions, and in response to engineering trades. Protection needs assessment is conducted repeatedly throughout the systems engineering processes.

[55] The protection need stems from the adverse impact should an asset be lost, compromised, replaced, modified, or degraded in any manner. How and why the loss occurs and the likelihood that the loss occurs is determined by the threat, vulnerability, and risk assessments. The protection needs assessment is what provides the scope for the other assessments that support security risk management.

There are relationships between the protection needs assessment and other assessments that support security risk management. The relationships determine when a change in the results of one assessment dictates the need to revisit the related assessments. Threat and vulnerability assessments combine to determine how a particular loss mode can occur and the potential for the loss to occur. As the architectural design matures and after the system is placed into operation, additional vulnerability information becomes available. These vulnerabilities can be associated with: (i) the architectural design; (ii) implementation decisions; (iii) the placement of protective measures in the system architecture and how those measures are used and interact; and (iv) the processes and procedures that are employed as protective measures. This information may expose certain vulnerabilities that translate to loss modes that were unforeseen during the protection needs assessment. The identification of a potential new loss mode warrants a review of the protection needs assessment results to ensure that the loss mode is properly assessed and that the severity of such a loss mode and the priority associated with that loss mode is reflected in the protection needs assessment results. Similarly, as new threat information becomes available, the initial protection needs assessment may have to be revised to address the new loss modes that are associated with changes in threat sources and threat events. Changes in the criticality, value, exposure, or importance of an asset may impact the threat, vulnerability, and risk assessments. Any change to the set of assets requiring protection requires an updated threat and vulnerability assessment to ensure that severity and likelihood of impact results and conclusions are complete with respect to the set of assets requiring protection.

### Threat Assessment

A *threat assessment* is the method used to identify and characterize the threats anticipated throughout the life cycle of the system. As a component of security risk management, the threat assessment has a close relationship with vulnerability assessment. It is the intersection of a threat event (i.e., malicious attack, non-malicious incident, accident, error, device fault/failure, natural or man-made disaster) and a vulnerability that results in the likelihood of harm to the system and that harm may translate to a negative impact on the mission/business. As the system design matures and the system is placed into operation, there will be greater insight into new and existing threats and vulnerabilities. The threat assessment is then revisited to ensure that all relevant threat sources and events are characterized and included in the scope of subsequent risk assessments. Figure 11 illustrates the key components of the threat assessment.

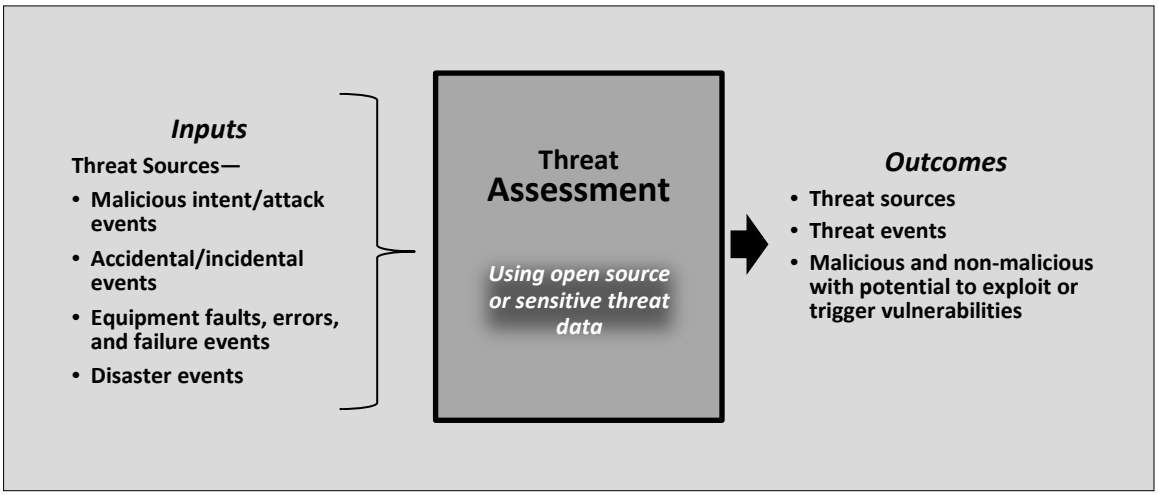


**FIGURE 11: KEY COMPONENTS OF THREAT ASSESSMENT**

The threat assessment also has a relationship to the protection needs assessment. The protection needs assessment determines the scope and focus of the threat assessment. The protection needs assessment identifies asset importance and severity of loss independent of threat. However, there can be cases where the threat assessment can offer insight into the susceptibility of an asset that was otherwise determined to be sufficiently protected, or for which the assigned priority requires adjustment (higher or lower). Additionally, if the protection needs assessment modifies the set of assets requiring protection, the threat assessment is revisited to ensure traceability to all assets. A cross-check between the threat assessment and protection needs assessment helps to ensure that: (i) the threat assessment is complete relative to the set of assets requiring protection; and (ii) the protection needs assessment did not overlook assets or fail to properly rank and prioritize the assets requiring protection.

### Vulnerability Assessment

A *vulnerability assessment* is the method used to identify and characterize the weaknesses and deficiencies that could be exploited or triggered by threat events throughout the system life cycle. As a component of security risk management, vulnerability assessment is closely related to threat assessment. It is the intersection of a threat event and a vulnerability (i.e., weakness/deficiency in technology components, physical components, processes, or procedures) that results in harm to the system—where such harm may subsequently translate into an adverse impact or negative consequences on the mission/business. As the architectural design matures and the system is placed into operation, there is greater insight into new and existing threat sources, threat events, and vulnerabilities. The vulnerability assessment is then revisited to ensure that all relevant vulnerabilities have been identified and assessed relative to the updated threat environment. Figure 12 illustrates the key components of the vulnerability assessment.

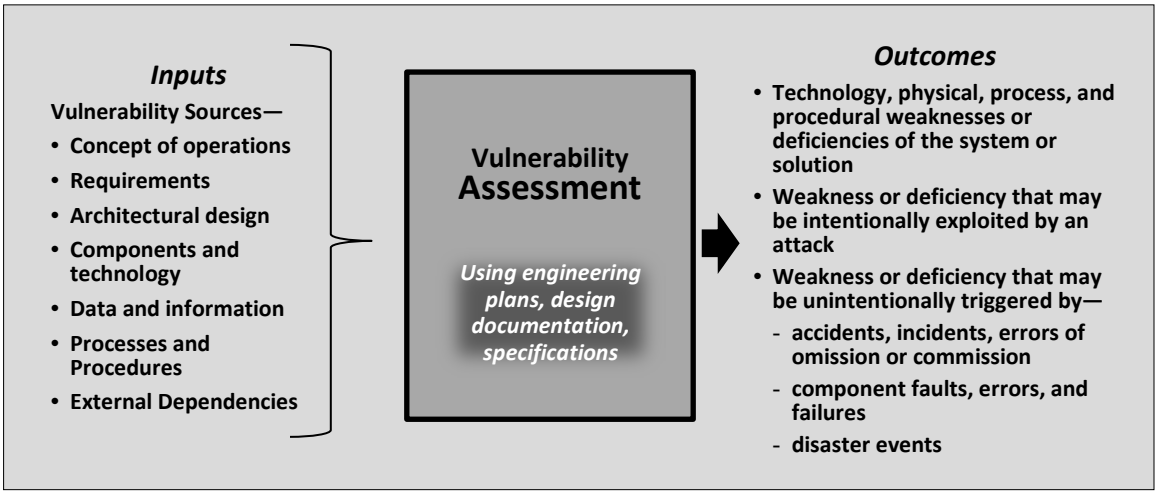


**FIGURE 12: KEY COMPONENTS OF VULNERABILITY ASSESSMENT**

In the same manner as the threat assessment, the vulnerability assessment also has a relationship to the protection needs assessment. The protection needs assessment determines the scope and focus of the vulnerability assessment. If the protection needs assessment modifies the set of assets requiring protection, the vulnerability assessment is revisited to accurately reflect the weaknesses and deficiencies associated with those assets. Likewise, the vulnerability assessment results are cross-checked with the protection needs assessment results to ensure that the assets requiring protection are not overlooked or improperly prioritized.

### System Security Risk Assessment

A *system security risk assessment* is the method used to conduct analyses and assessments to: (i) provide an enumeration of system security risks; and (ii) determine for each identified risk, its severity, likelihood of occurrence, and relative ranking/priority for risk treatment. The system security risk assessment is informed by the results of the protection needs assessment, the threat assessment, and the vulnerability assessment. Systems security risk assessment determines: (i) the likelihood and consequences resulting from a threat event exploiting or triggering a vulnerability; (ii) the impact to system elements, data, and information; and (iii) the system-level impact. The system security risk assessment is conducted in consideration of the system's intended use and configuration in the environment of operation. System-level impact includes: (i) degradation or loss of availability of function; (ii) degradation or loss of integrity of function, data/information; and (iii) unauthorized infiltration or exfiltration of data/information (to include acquiring the knowledge of the existence of specific system capabilities, configurations, and vulnerabilities). The system-level impact informs the broader risk assessment that identifies risk relative to the stakeholder's mission/business objectives/concerns and enables stakeholders to make informed risk treatment decisions. Figure 13 illustrates the key components of the system security risk assessment.

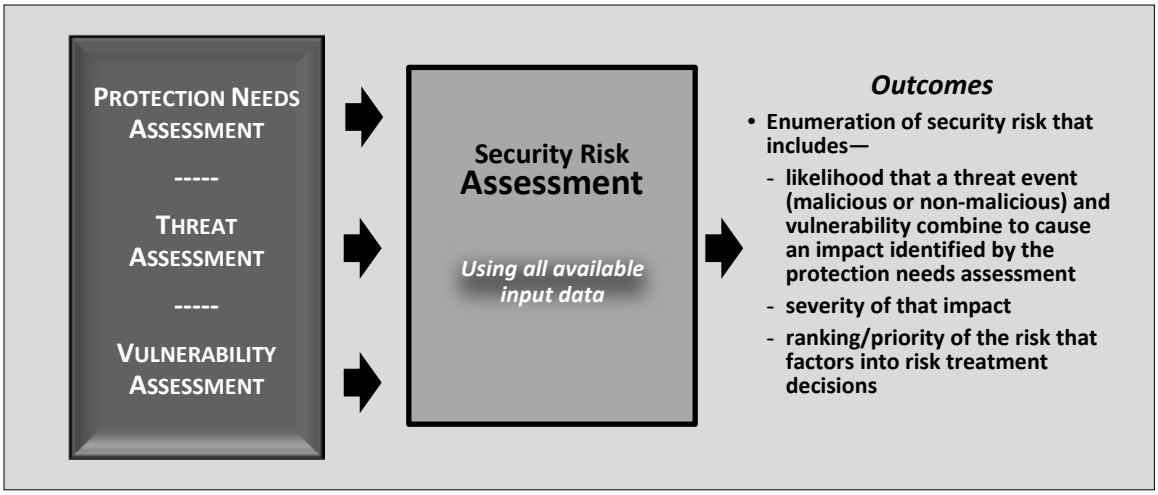


**FIGURE 13: KEY COMPONENTS OF SYSYEM SECURITY RISK ASSESSMENT**

System security risk assessment is accomplished continuously as part of developmental and field engineering activities. The initial system security risk assessment establishes a baseline for the continuous security risk treatment that includes the cycle of making cost-effective engineering trade decisions to identify and institute effective protective measures, assessing the effectiveness of those protective measures, and determining the new security risk posture. As part of their risk management responsibilities, stakeholders determine whether the residual risk can be accepted or if further security risk treatment is required. The user/owner/operator/sustainment communities are involved in the final assessment and determination of what constitutes acceptable security risk and must be informed to ensure that they are able to interpret and use the results of the security risk assessment as part of their organizational risk management processes.

### Security Risk Treatment

*Security risk treatment* is the method used to identify feasible security risk mitigation options and to develop risk treatment plans. Protective measure trades are part of risk treatment and focus on

options for mitigating risk by employment of specific protective measures. Risk treatment: (i) identifies candidate protective measures; (ii) provides information about the overall effectiveness, cost/benefit, and vulnerability associated with those measures; (iii) conducts trade space analyses to recommend a course of risk mitigation action; and (iv) makes the determination of which of the candidate options are to be employed. Security risk treatment is conducted as part of technical systems security engineering activities to analytically select cost-effective protections and to plan for the incorporation of the selected protective measures into the total-system security concept.[56]

The employed protective measures may eliminate or reduce vulnerabilities or they may contain the impact resulting from the exploitation or triggering of vulnerabilities. They may also serve to monitor the actions and behavior of threat sources or to monitor system behavior such that it is possible to predict or detect conditions indicative of threat events that constitute malicious exploitation or non-malicious triggering of a vulnerability. Protective measures are crafted from: (i) the application of protection strategies, methods, techniques, tools, and technologies; (ii) the application of security design principles and concepts; and (iii) adherence to prescribed processes, best practices, and methods. Protective measures may also present a level of risk due to the inherent vulnerabilities they contain. Therefore, the employment of a protective measure may introduce or expose risk that would not otherwise exist. It is possible that the employment of a protective measure can reduce risk in one context while increasing risk in some other context. Figure 14 illustrates the key components of security risk treatment.

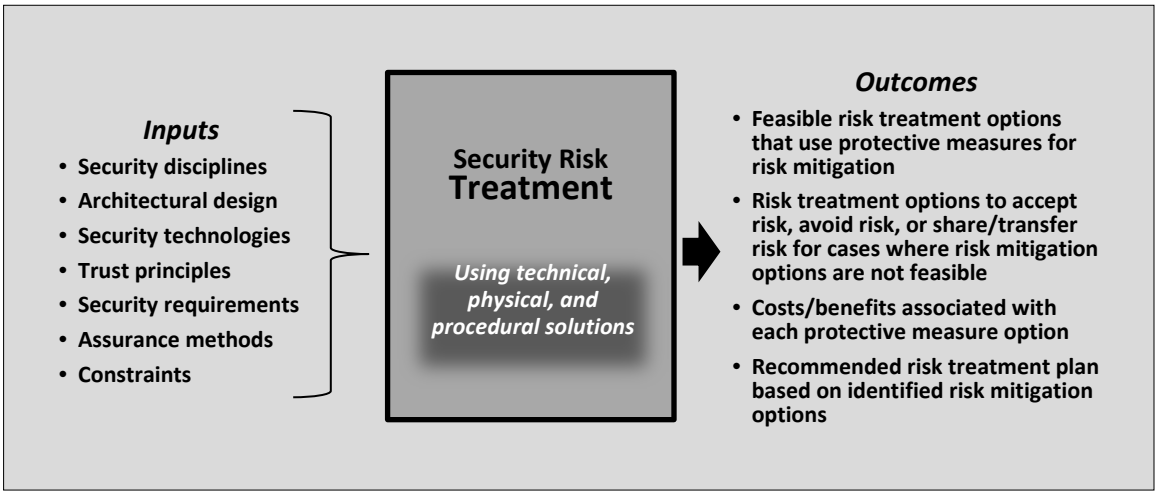


**FIGURE 14: KEY COMPONENTS OF SECURITY RISK TREATMENT**

In determining the cost/benefit of a protective measure, all relevant costs are considered. The costs associated with a protective measure include: (i) the cost to acquire, develop, integrate, operate, and sustain the measure over the system life cycle; (ii) the cost as a measure of impact to system performance; (iii) the cost of documentation and training; and (iv) the cost of assurance. The cost of assurance includes the cost to obtain evidence and to conduct analysis required by assurance requirements and the cost to provide reasoning that substantiates claims that sufficient trustworthiness has been achieved.

The benefit derived from a protective measure is determined by: (i) the overall effectiveness of the measure in providing the protection allocated to it; (ii) the trustworthiness that can be placed

[56] The employment of protective measures is the risk treatment option that may *mitigate risk* and/or *share risk.*

on the measure; and (iii) the residual risk associated with the use of the measure, given the value, criticality, exposure, and importance of the assets that the measure protects. It may be the case that an optimal cost/benefit is realized from the employment of a combination of less costly protective measures rather than employment of a single cost-prohibitive protective measure. It may also be the case that the adverse performance impact on the system may preclude the use of a particular protective measure. Consideration is given to alternate architectural design options that can meet the performance and protection needs or that provide an acceptable balance between meeting performance needs while providing protection that remains within risk tolerance.

Ultimately, the purpose of security risk treatment is to achieve residual risk that is within the specified risk tolerance of stakeholders. While the preference for risk treatment is given to employment of protective measures, when doing so is not feasible or cost-ineffective, alternative risk treatment options include: (i) sharing risk with an organization that is in a better position to provide the required mitigations; (ii) avoiding risk to eliminate the threat/vulnerability or the adverse impact/consequence (e.g., change the concept of operations or defer implementation of a capability); or (iii) accepting risk, which requires instituting methods or techniques to monitor the conditions that lead to the risk being accepted.

***Determining Appropriate Levels of Protection for Assets***

All organizational assets require *some* level of protection—that is, a minimum level of protection constituting security *due diligence*. After providing the minimum level of protection, those assets considered critical, high value, or high importance are then provided additional protections. The purpose of determining the criticality, value, and importance of assets is not to pick and choose which assets to protect; rather, it is to determine which assets require greater protection above that level of minimum protection.

CHAPTER THREE

# THE PROCESSES

LIFE CYCLE-BASED SYSTEMS SECURITY ENGINEERING PROCESSES

This chapter describes a set of systems security engineering processes. These processes are aligned with International Standards ISO/IEC 15288 and IEEE Std. 15288, *Systems and software engineering – System life cycle processes*.[57] The initial scope of this publication is limited to the Technical Processes described in ISO/IEC/IEEE 15288.[58] The systems security engineering processes: (i) leverage the concepts, terms, principles, and practices of systems engineering to facilitate consistency in application as part of a comprehensive, broad-based systems engineering effort; and (ii) articulate the roles and responsibilities of the systems security engineer. The systems security engineering processes incorporated into each stage of the system life cycle, establish an approach to formally or informally execute a set of well-defined security-relevant activities as part of a systems engineering effort to ensure that organizational *protection needs* are addressed by the delivered system. The processes can be employed to provide security contributions to specific engineering processes or as a guide for the engineering that is necessary to achieve trustworthy systems.[59] The descriptions of the systems security engineering processes assume that sufficient time, funding, and human/material resources are available to ensure a complete application of the processes within a comprehensive systems engineering effort.

Each of the eleven technical processes contains a set of *activities* and *tasks* that produce *outcomes* used in subsequent processes.[60] Process outcomes combine to deliver a sufficiently trustworthy system and a comprehensive body of evidence that is used to: (i) provide design assurance; (ii) substantiate the trustworthiness of the system; (iii) provide inputs to other processes associated with delivering the system; (iv) determine mission/business risk based on the use of the system; (v) help stakeholders decide which operational constraints may be necessary to mitigate residual risk; and (vi) support the system throughout its life cycle. While all of the technical processes from ISO/IEC/IEEE 15288 are addressed from the context of systems security engineering, only those activities and tasks that are security-relevant are included in this publication. Activities and tasks have also been added to the systems and software engineering processes in situations where the standard was not sufficiently robust to address the range of activities and tasks needed for a comprehensive systems security engineering process.

[57] ISO/IEC/IEEE 15288 establishes a common framework for describing the engineering life cycle processes for systems created by humans. Such man-made systems typically include one or more of the following: hardware, software, data, humans, processes, procedures, facilities, materials and naturally occurring entities. The standard defines a set of processes that can be applied concurrently, iteratively, or recursively at any level in the hierarchy of a system's structure and throughout the system life cycle.

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

[59] The concepts and principles employed in the systems security engineering processes can be applied to the engineering of a complex security mechanism, a system, or a complex system-of-systems. While the complex mechanism can be addressed by a small team, the engineering of the complex system-of-systems may require a hierarchical organizational structure with multiple coordinating and interacting teams, all reporting to a lead systems engineer. The processes can be tailored accordingly to facilitate their effectiveness.

[60] Outcomes from processes can also serve to inform other processes external to the engineering effort, such as organizational processes for independent verification and validation (IV&V), risk management, training, and sustainment.

The systems security engineering processes identify the security-relevant parts of the system and provide security-focused enhancements to the activities defined by the systems engineering effort. Thus, the security-enhanced process activities provide a security-focused interpretation of the system. Security-focused analyses examine the system elements, the interconnections between those elements, and the environment in which the system operates. These analyses identify the security-relevant portions of the system, the trust relationships among system elements, and the overall levels of assurance and trustworthiness in the system. The resultant system is viewed as a cohesive entity, potentially composed of multiple systems, services, mechanisms, policies, and procedures that may be distributed across one or more system elements.

The systems security engineering processes may be *tailored* in their application, providing the needed flexibility and agility for use in a wide variety of systems engineering efforts supporting diverse communities of interest, including, for example, manufacturing, transportation, defense, finance, energy, and healthcare. Tailoring can include: (i) altering the defined execution sequence of processes and activities for more effective application; (ii) supplementing the process activities in response to unique requirements or other circumstances; and (iii) completing the engineering effort without performing all of the individual processes and activities. Process tailoring may be required due to: (i) the stage of the system life cycle; (ii) the size, scope, and complexity of the system; (iii) unique or special-case requirements; or (iv) the need to be able to accommodate specific methods and technologies used to develop the system. Tailoring may also be appropriate in cases where the activities of different processes might overlap or interact in ways not defined in this document.[61] Tailoring the systems security engineering processes allows the systems security engineer to:

- Optimize the application of the processes in response to technological, programmatic, process, procedural, system life cycle stage, or other constraints;
- Facilitate the application of the processes within the system development processes, methodologies, and models (e.g., agile, spiral, waterfall);
- Accommodate the concurrent application of the processes by sub-teams focused on different parts of the same engineering effort; or
- Accommodate the need for iteration of process activities to resolve issues and respond to changes that occur during the engineering efforts.

Each systems security engineering process description has the following format:

- Purpose. The purpose section identifies the primary goals and objectives of the process and provides a summary of the security-focused activities conducted during the process.
- Outcomes. The outcomes section describes what is achieved by the completion of the security-enhanced process and the information/evidence[62] generated by the process.[63]

[61] For example, the engineering team may need to initiate a system modification in a relatively short period of time in order to respond to a serious security incident. In this situation, the engineering team may only informally consider each process rather than formally executing each process. It is essential that any system modifications continue to support the stakeholder's security needs. Without this system-level perspective, modifications could fix one problem while introducing others. See Appendix E, Scenarios, for specific examples that address this situation.

[62] Information/evidence generated as a process outcome is not necessarily produced in the form of a document. Such information/evidence can be conveyed in the most effective manner as set forth by the stakeholders/engineering team.

[63] Information generated may flow into a subsequent process or support processes that are associated with the systems security engineering process.

- Activities and Tasks. The activities and tasks section provides a description of the actual work performed during the process including the specific security-focused enhancements to the activities/tasks.

The activities and tasks conducted during the execution of any process may be repeated, in whole or in part, to resolve any gaps and issues identified. Any iteration between processes requires additional scrutiny to ensure that changes to the outcomes of previously executed processes are properly incorporated into the activities and tasks of the current process. It may also be the case that some parts of the engineering effort can move ahead to the next process while others may continue to be worked in the current and preceding processes. The impact of dividing the engineering effort is assessed to ensure that risk is properly understood and managed.

Systems security engineering activities eliminate or reduce vulnerabilities and minimize or constrain the impact of exploiting/triggering vulnerabilities. This in turn reduces the susceptibility of systems to a variety of simple and complex threats including physical and cyber attacks, natural disasters, structural failures, and errors of omission and commission. Such reduction is accomplished by properly understanding the organization's protection needs and subsequently employing sound security architectural design principles and concepts through the engineering processes. These processes, if properly carried out, result in stronger, more penetration-resistant and resilient systems and a measurable level of assurance and trustworthiness to more effectively manage mission/business risk.

The following naming convention is established for the systems security engineering process to help identify the constituent processes, activities, and tasks. Each process is identified by a two-character designator (e.g., SR is the designator for the Stakeholder Requirements Definition Process). Table 1 provides a listing of the eleven technical systems engineering processes and their associated two-character designators.

**TABLE 1: PROCESS NAMES AND DESIGNATORS**

| ID | PROCESS NAME | ID | PROCESS NAME |
|---|---|---|---|
| SR | Stakeholder Requirements Definition | TR | Transition |
| RA | Requirements Analysis | VA | Validation |
| AD | Architectural Design | OP | Operation |
| IP | Implementation | MA | Maintenance |
| IN | Integration | DS | Disposal |
| VE | Verification | | |

Activities and tasks in each systems security engineering process are uniquely identified using a two-character process designator plus a numerical designator. For example, the first activity in the *Stakeholder Requirements Definition Process* is designated SR-1. The first two tasks within SR-1 are designated SR-1-1 and SR-1-2. The unique identification of activities and tasks within the systems security engineering process supports the traceability of requirements, an important characteristic of any development effort.

Each task description is supported by a *supplemental guidance* section which provides additional information on factors relevant to the successful execution of that task. In addition, a *references* section provides a list of pertinent publications associated with the tasks within an activity. Such references can include, for example, security-related standards, guidelines, best practices, or other

publications deemed important to completing the activity. The following example illustrates the task structure within an activity associated with a particular systems engineering process:

SR-2-5: Specify the stakeholder security requirements and identify the functions that relate to the mission/business protection needs of the stakeholders.

Supplemental Guidance: The stakeholder security requirements include all areas of system security and all areas of assurance that are tied to system security including, for example: (i) computer, communications, emissions, operations, transmission, and physical security; (ii) hardware, software, firmware, information, and supply chain assurance; and (iii) protection against reverse engineering. The stakeholder security requirements comprise the functions that provide the confidentiality, integrity, and availability protections within the system, and protections for services provided by the system. The stakeholder security requirements and functions address security both as a protection capability and as a system quality property.

References: ISO/IEC 15408; FIPS Publication 200; NIST Special Publications 800-30, 800-53.

Figure 15 highlights the eleven ISO/IEC/IEEE 15288 technical systems engineering processes and the intent for their application across all system life cycle stages.

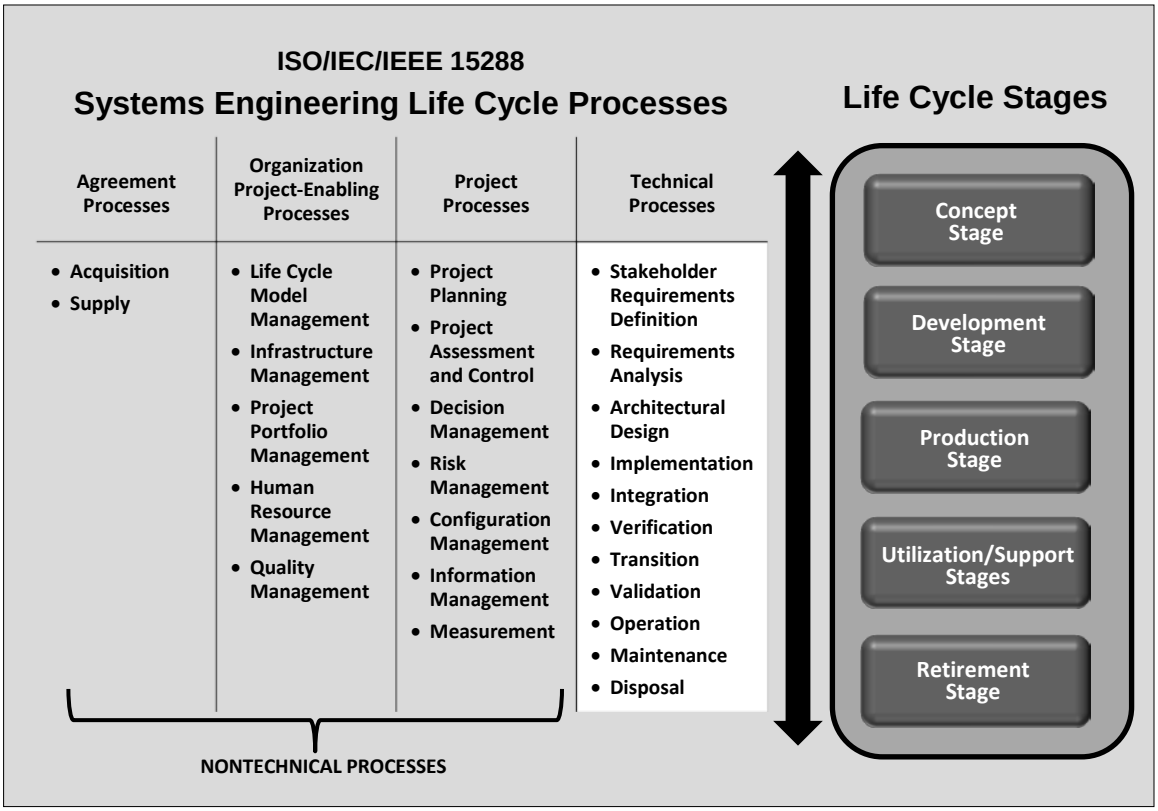


**FIGURE 15: SYSTEMS ENGINEERING PROCESSES AND ASSOCIATED LIFE CYLE STAGES**

The term *engineering team* in this publication refers to the individuals on the systems engineering team with security-related responsibilities, systems security engineers that are part of the systems engineering team, or a combination thereof. The intent is to focus on the security-related elements of the systems engineering processes, activities, and tasks rather than assigning specific labels to the individual members of the team.

The remaining sections in this chapter describe the security-related enhancements to the eleven *Technical Processes* defined in ISO/IEC/IEEE 15288. These security-related enhancements that have been integrated into the systems and software engineering processes in the form of activities and tasks extend the scope of the processes to include systems security engineering.[64]

### *Systems Engineering Perspectives*

Systems engineering efforts are a complex undertaking that involves close coordination among the engineering team and organizational stakeholders throughout the stages of the system life cycle. To achieve such coordination, systems engineering is composed of *development engineering* and *field engineering* teams, each with specific roles and responsibilities. These two teams coordinate and exchange information during the execution of the eleven technical systems engineering processes described in Chapter Three.

Systems engineering does not stop once a system completes development and is transitioned to the environment of operation for day-to-day operational use. Field engineering (also known as *sustainment engineering*) complements development engineering to provide for full life cycle engineering coverage of systems. Field engineering activities provide support to the operations, maintenance and sustainment, and disposal stages of delivered systems. Field engineering teams may be dispatched to operational sites or may be co-located at operational sites and maintenance depots to provide ongoing systems engineering support to operational organizations.

The systems engineering processes of *Operation* (**OP**), *Maintenance* (**MA**), and *Disposal* (**DS**) are not intended to prescribe the day-to-day operations, maintenance, or disposal activities employed by organizations. Nor are field engineering teams or personnel responsible for the execution of operations, maintenance, or disposal activities. Rather, these systems engineering processes accomplish the engineering component of planning for the operations, maintenance, and disposal life cycle stages of the system, and contribute to the system requirements, architectural design, and development of best practices, procedures, and training in support of those system life cycle stages. Field engineering teams work alongside the operations and maintenance personnel to assist in the collection of information in support of the investigation and analysis of events and circumstances associated with failures, incidents, attacks, accidents, and other cases where there is demonstrated or suspected nonconformance to the system or its specified behavior.

Field engineering teams may also assist in the installation of planned modifications, upgrades, or enhancements to the system. The field engineering team applies all relevant systems engineering processes (including the **SR**, **RA**, **AD**, **IP**, **IN**, **VE**, **TR**, and **VA** processes) as necessary, while addressing field engineering issues. The field engineering teams may also consult with and provide feedback to the developmental engineering teams to ensure that lessons learned in the field are properly communicated: (i) to inform future development engineering efforts; and (ii) to help ensure that relevant improvements and modifications being made on future systems can be employed to systems in the field.

[64] The Technical Processes do not map explicitly to specific stages in the system life cycle. Rather, the processes may occur in one or more stages of the life cycle depending on the particular process and the conditions associated with the engineering effort. For example, the Maintenance Process includes activities that plan the maintenance strategy such that it is possible to identify constraints on the system design necessitated by how the maintenance will be performed once the system is operational. This example illustrates that the maintenance process is conducted prior to or concurrent with the Architectural Design process.

## 3.1 STAKEHOLDER REQUIREMENTS DEFINITION PROCESS

***Purpose***

"The purpose of the Stakeholder Requirements Definition Process is to define the requirements for a system that can provide the services needed by users and other stakeholders in a defined environment. It identifies stakeholders, or stakeholder classes, involved with the system throughout its life cycle, and their needs, expectations, and desires. It analyzes and transforms these into a common set of stakeholder requirements that express the intended interaction the system will have with its operational environment and that are the reference against which each resulting operational service is validated."



### Systems Security Engineering Purpose

Systems security engineering, as part of the *Stakeholder Requirements Definition Process*, defines stakeholder requirements for the protections incorporated into a system that provide sufficient and effective protection for user and other stakeholder assets given the threat events anticipated in the defined operating environment. Systems security engineering conducts security-focused requirements elicitation and analysis activities to identify stakeholders and stakeholder protection needs, expectations, and desires throughout the system life cycle and transforms such information into protection-oriented requirements (i.e., stakeholder security requirements).

### Systems Security Engineering Outcomes

The following *outcomes* can be expected from the successful execution of a security-enhanced Stakeholder Requirements Definition Process:

- Required characteristics and context of use of security services and operational security concepts are specified;
- Security-relevant constraints on a system solution are defined;
- Stakeholder security requirements are defined, are traceable to the stakeholders and their stated protection needs, and are incorporated into the overall stakeholder requirements;
- Stakeholder security requirements for validation and validation methods are identified;
- Asset Protection Model is developed;
- Preliminary security concept of operations is developed; and
- Key stakeholder concurrence is obtained.

### Systems Security Engineering Activities and Tasks

The following security-related *activities* are conducted as part of the Stakeholder Requirements Definition Process:

- Elicit stakeholder security requirements;
- Define stakeholder security requirements; and
- Analyze and maintain stakeholder security requirements.

SR-1: ELICIT STAKEHOLDER SECURITY REQUIREMENTS

SR-1-1: Identify the stakeholders who have an interest in or are responsible for the protection of the system throughout its life cycle.

Supplemental Guidance: Stakeholders include all persons, groups, and organizations that impact the system or are impacted by the system, including the protection aspects of the system. All stakeholders are identified, including specific roles and responsibilities relative to the systems engineering effort. The engineering team ensures that all security-relevant roles (e.g., information owners, mission/business owners, authorization officials, operations, training, and sustainment personnel) are included in the stakeholder identification task. The *key* stakeholders are a subset of the stakeholders that have decision-making responsibility: (i) associated with engineering and risk trade decisions; (ii) for authorization decisions associated with engineering milestones; and (iii) for system acceptance and use authorization decisions. Key stakeholders and their decision-making responsibilities may change as the systems engineering effort progresses through the individual processes. The engineering team identifies key stakeholders for each process and their specific responsibility for that process prior to performing activities in that process.

SR-1-2: Elicit stakeholder security requirements from the identified stakeholders with protection interests or responsibilities related to the system.

Supplemental Guidance: The engineering team obtains information from stakeholders to determine the protection needs necessary to support the mission/business. The team obtains this information from documentation and through discussions with stakeholders and uses the information to formalize stakeholder security requirements. Stakeholders do not necessarily have the ability to speak to their protection needs in the same manner as they would be prepared to speak about their other needs. Therefore, the engineering team leads the discussion in a way to get the stakeholders in the right mindset and context to speak about protections. Moreover, the engineering team must be prepared to do that introspective thinking on behalf of the stakeholders to extract the protection needs, document those needs, and then transform the needs into stakeholder security requirements.

Stakeholders provide information in the form of needs, desires, objectives, expectations, assumptions, and constraints. Stakeholders may provide information formally (e.g., specific objectives, specific requirements, security controls, standards, policies, directives, and regulations) or informally (e.g., abstract statements of goals). Information elicited from the stakeholders may be inconsistent, ambiguous, conflicting, or incomplete. The engineering team resolves these issues during the elicitation activity, if possible, by presenting the issues to the stakeholders, asking follow-up questions, and having stakeholders provide additional information and clarification.

The information required to determine stakeholder security requirements varies based on the scope of the system. If one element or capability of an existing operational system is to be upgraded (e.g., audit management system, continuous monitoring capability), the scope may be narrow. If an entire system is required to provide a new functional capability (e.g., a new aircraft with supporting ground systems or adding a new business function, product line, or service), then the scope may be broad. In both cases, the engineering team obtains the same type of information for analysis and determination of stakeholder security requirements.

The elicitation of protection needs also requires stakeholders to provide input to support the analyses regarding the criticality, value, importance, and exposure of assets and the potential adverse impact or consequences to the mission/business resulting from loss of confidentiality, integrity, or availability of such assets. This input may be obtained from an organization-specific prioritization of assets relative to mission/business objectives or may be derived from the results of a security categorization activity defined by policies, directives, or standards. Stakeholder input is important to ensure that the engineering team analyses used to develop stakeholder security requirements reflect the organization's mission/business priorities and assurance objectives. The results of the analyses also support engineering trade analyses, risk assessment, risk treatment, and new, changed, or deleted requirements in the stakeholder requirements baseline.

The engineering team ensures that security relevant information is obtained in the following areas:

- Mission/business
  - Environment of operation of the mission/business;
  - Processes, procedures, and interactions that govern how the organization performs its mission/business;
  - Roles and responsibilities of personnel that use or rely on the system;
  - Placement of the system within the organization (i.e., physical/logical placement, infrastructure placement, etc.);
  - Interactions with other organizations; and
  - Criticality of organizational functions defined for each mission/business line.
- Use of the system
  - Method of using the system to support the mission/business;
  - Interactions with other systems within the organization; and

  - Interactions with other organizations and systems, services, and infrastructures.
- Information
  - Identification of information owners and the information required to support the mission/business;
  - Method of using information to support the mission/business;
  - Sensitivity of information and concerns associated with its use and dissemination;
  - Identification of legal, regulatory, privacy, or other requirements that address information protection, use, and dissemination;
  - Information criticality and prioritization in supporting the mission/business; and
  - Impact to the mission/business, the organization, and other organizations if the information is compromised, damaged, or becomes inaccessible.
- System elements not part of the system-of-interest
  - Identification of systems, infrastructures, and services used to support the mission/business;
  - Method of use for systems, infrastructures, and services to support the mission/business;
  - Criticality of systems, infrastructures, and services used to support the mission/business; and
  - Impact to the mission/business, the organization, and other organizations if systems, infrastructures, and services are compromised, damaged, or become inaccessible.
- Threats/Hazards
  - Identification of potential threat sources (i.e., natural disasters, structural failures, cyber and physical attacks, or errors of omission and commission) to the mission/business;
  - Identification of threat events and the potential adverse impact to the mission/business; and
  - Continuity of operations plans, procedures, and protections in response to threat events (including hazards).
- Compliance
  - Policy, legal, and regulatory requirements and mandates;
  - Processes to be followed (e.g., acquisition, risk management, independent verification/validation, assurance, assessment, authorization, software and hardware development); and
  - Agreements, arrangements, and contracts for services provided to or received from external organizations.

References: None.

### SR-2: DEFINE STAKEHOLDER SECURITY REQUIREMENTS

#### SR-2-1: Define the security-relevant constraints on the system.

Supplemental Guidance: Security-relevant constraints may derive from existing agreements, management decisions, and/or technical decisions. The engineering team obtains security-relevant information for the following potential constraints on the security and non-security aspects of the implementation:

- Technical, operational, authorization, and other constraints;
- Required interactions with systems, services, and infrastructures;
- Required use of defined resources and staff;
- Stakeholder-defined use of specific architectural or computing models;
- Mandated use of specific products, services, and technologies; and
- Considerations of and limitations for size, weight, power, or other environmental factors.

The engineering team identifies, documents, and preserves for ongoing use throughout the engineering processes, the assumptions, constraints, risk tolerances, and engineering working notes used to determine the stakeholder security requirements. The Asset Protection Model described in Task 2-4 is the primary systems security engineering artifact for the information used to develop the stakeholder security requirements.

#### SR-2-2: Identify the interaction between users and the system including any services required for the operational support of the system.

Supplemental Guidance: The interaction between users and the system provides the context for the development of a preliminary security concept of operations (CONOPS), which serves as an input to determine stakeholder protection needs. The security CONOPS provides the security-influenced philosophy for the use of the system to protect the mission/business including mission/business processes and assets in a manner that achieves operational objectives. It also includes services that support operations, sustainment, and training. The engineering team develops the security concept of operations as part of the system concept of operations to ensure that the two CONOPS are consistent, compatible, and tightly integrated. The team performs a least privilege analysis to determine the attributes of security

policies governing access to and the use of the functions, information, systems, infrastructures, and services needed to support the mission/business objectives.

Least privilege analysis is a necessary input to the Asset Protection Model described in Task SR-2-5. This analysis is used to determine the minimum set of privileges required by individuals, programs, processes, and services to achieve their stated purpose in support of the mission/business. The analysis avoids influences by planned or existing system context, design, or implementation. The analysis considers security domain abstractions, the different types of active entities and their abstractions (e.g., individuals, users, programs, processes, services), and other security-relevant information or mission/business abstractions. Least privilege analysis also includes how each active entity and its abstractions utilize information and perform operations in support of the mission/business. Operations are defined in the context of the function of the active entity. Typical operations on data or information include read, write, and delete. However, operations may include start or stop a process, open or close a valve, increase or decrease bandwidth on a communication channel, or increase or decrease the power to a generator. And finally, the analysis generates information that is used to define a security policy that is independent of technology influences.

SR-2-3: Identify and assess threats to mission/business assets.

Supplemental Guidance: The engineering team determines how threats in the environment of operation potentially impact the information, systems, infrastructures, and services relied upon to perform mission/business processes and functions. Threat assessment is the method to identify and characterize the threats anticipated throughout the life cycle of the system. The threat and assessment results along with a determination of adverse consequences (or impacts) are key elements of a risk assessment. It is the intersection of a threat event (i.e., malicious attack, non-malicious incident, accident, error, or device fault or failure, natural or man-made disaster) and a vulnerability that results in harm to the mission/business through the use of the system. As the system design matures and the system is placed into operation, the engineering team has greater insight into existing vulnerabilities and can identify new vulnerabilities. The team can revisit the threat assessment as new information becomes available.

The threat assessment also has a relationship to the protection needs assessment. The protection needs assessment determines scope and focus when conducting the threat assessment. The protection needs assessment identifies asset importance and severity of loss independent of threat. However, there may be instances where the threat assessment can offer insight to the susceptibility of an asset that stakeholders considered to not require protection or that had a priority that should have been higher. Additionally, if the protection needs assessment modifies the set of critical assets, the engineering team revisits the threat assessment to consider the susceptibility of the new set of critical assets to the current threats. A crosscheck between the threat assessment and protection needs assessment helps to ensure that the threat assessment is complete relative to the set of critical assets, and helps to ensure that the protection needs assessment did not overlook critical assets or fail to properly rank and prioritize the assets requiring protection.

SR-2-4: Determine mission/business asset protection needs.

Supplemental Guidance: The engineering team conducts a protection needs assessment to identify stakeholder protection needs for the assets that support the mission/business. Mission/business assets may be characterized as either tangible or intangible assets. Tangible assets are physical in nature and include physical elements of the environment of operation (e.g., structures, utility infrastructures) and hardware elements of systems, network, telecommunication infrastructure, communications, and components and mechanisms. Intangible assets are not physical in nature and include data, information, firmware, and software, mission/business processes, services, and functions. Data and information assets include data and information required to execute mission/business processes and for system operation and management, sensitive and proprietary data (e.g., classified information, controlled unclassified information, critical program information, privacy information, trade secrets, intellectual property), and all forms of documentation associated with the system. Additionally, intangible assets include the image and reputation of an organization. Tangible and intangible assets directly perform or contribute to performing mission/business functions.

The engineering team describes the protection needs obtained from stakeholders for tangible and intangible assets in an Asset Protection Model. This model provides the foundation for the detailed analysis to determine stakeholder security requirements, and serves as a means to scope and focus ongoing threat, vulnerability, and risk assessments. In addition, the model provides a protection management view of mission and business capability, function, component, process, information, and technology assets. For each asset, supporting information and attributes reflect the role of the asset, the impact of loss of the asset, the importance of the asset (e.g., criticality, sensitivity, value), the exposure of the asset, and the protections required for the asset (e.g., confidentiality, integrity, availability). The Asset Protection Model: (i) identifies all assets that are candidates for protection; (ii) is independent of any planned or existing system context, design, or implementation; (iii) contains a relative prioritization of assets that identifies and distinguishes more critical assets from less critical assets; (iv) supports engineering trades for determining specific asset protection mechanisms; and (v) supports risk management decisions for allocation of human and material resources for risk treatment (i.e., risk response).

The Asset Protection Model contains the following asset types:

- Data and information;
- Sensitive, proprietary, privacy, and personally identifiable data and information;
- Components;
- Infrastructure;
- Systems, system-of-systems;
- Function;
- Capability;
- Provision of service;
- Processes, procedures;
- Intellectual property; and
- Technological, competitive, and combatant advantage.

Organization-specific terms may be used to further distinguish or differentiate details of these common asset types. The Asset Protection Model uses input from the threat and least privilege analyses conducted as part of stakeholder security requirement definition. The results of those analyses are also captured in the model.

SR-2-5: Specify the stakeholder security requirements and identify the functions that relate to the mission/business protection needs of the stakeholders.

Supplemental Guidance: The stakeholder security requirements include all areas of system security and all areas of assurance that are tied to system security including, for example: (i) computer, communications, emissions, operations, transmission, and physical security; (ii) hardware, software, firmware, information, and supply chain assurance; and (iii) protection against reverse engineering. The stakeholder security requirements comprise the functions that provide the confidentiality, integrity, and availability protections within the system, and protections for services provided by the system. The stakeholder security requirements and functions address security both as a protection capability and as a system quality property.

References: ISO/IEC 15408; FIPS Publication 200; NIST Special Publications 800-30, 800-53.

SR-3: ANALYZE AND MAINTAIN STAKEHOLDER SECURITY REQUIREMENTS

SR-3-1: Analyze the stakeholder security requirements.

Supplemental Guidance: The engineering team analyzes the set of stakeholder security requirements for completeness, consistency, and clarity. The team identifies any requirements that are incomplete, ambiguous, or in conflict with other requirements, and any gaps and omissions in the requirements.

SR-3-2: Resolve any conflicts, inconsistencies, or gaps in the stakeholder security requirements.

Supplemental Guidance: The engineering team resolves security requirements problems by addressing issues such as conflicts, inconsistencies, and gaps in the stakeholder security requirements or in the broader system requirements. The team addresses security requirements problems with appropriate stakeholders to ensure consistency and compatibility among all requirements. When resolving security requirements issues, stakeholders weigh their intent to achieve a specific operational capability against the cost of the protections required to secure that operational capability including any identified constraints. These costs include, but are not limited to: (i) financial; (ii) schedule; (iii) human/material resource availability and suitability; (iv) development, operations, sustainment, and training; and (v) assurance and practicality. Stakeholders also determine the mission/business impact and risk associated with security requirements that cannot be implemented. Stakeholders may decide to remove certain requirements from the requirements baseline based on issues cited during this process or any other process. The engineering team modifies the requirements baseline to reflect new, modified, and deleted stakeholder security requirements. Additionally, any change to the stakeholder requirements signifies the need to reassess protection needs and determine if any subsequent changes are required to the stakeholder security requirements.

SR-3-3: Convey stakeholder security requirements to stakeholders to ensure that their protection needs and expectations have been adequately captured and expressed.

Supplemental Guidance: The engineering team ensures that stakeholders understand and are satisfied with the security requirements derived from the protection needs and that the security requirements are correctly expressed. In some

cases, the security requirements may not be obvious to stakeholders but have been incorporated into the system-level requirements based on the protection needs articulated by the stakeholders and the understanding of the engineering team of the capability required to protect the assets defined by the stakeholders. Protection needs include considerations for the security-related aspects of design, development, operations, sustainment, training, human factors, and safety.

SR-3-4: Record and maintain stakeholder security requirements in a form suitable for requirements management throughout the system life cycle.

Supplemental Guidance: The engineering team documents stakeholder security requirements and ensures that such requirements: (i) are treated as first-order requirements; (ii) become part of the requirements baseline; (iii) are traceable to the source of stakeholder protection needs and associated protection capabilities; and (iv) are part of the exit criteria to satisfy engineering process milestones. The team maintains traceability between the stakeholder requirements and the various forms of expression used by stakeholders to express their protection needs. The engineering team also documents and preserves for ongoing use throughout the engineering processes, the assumptions, constraints, risk tolerances, and engineering working notes used to determine the stakeholder security requirements. It is noted that the term *requirement* has a specific and formal meaning within the context of systems engineering and engineering efforts. In that context, a requirement is *only* that which is formally stated, validated, and captured in a *requirements baseline*.

References: None.

## 3.2 REQUIREMENTS ANALYSIS PROCESS

***Purpose***

"The purpose of the *Requirements Analysis Process* is to transform the stakeholder, requirement-driven view of desired services into a technical view of a required product that could deliver those services. This process builds a representation of a future system that will meet stakeholder requirements and that, as far as constraints permit, does not imply any specific implementation. It results in measurable system requirements that specify, from the supplier's perspective, what characteristics it is to possess and with what magnitude in order to satisfy stakeholder requirements."



### Systems Security Engineering Purpose

Systems security engineering, as part of the *Requirements Analysis Process*, transforms the stakeholder security requirements into the system security requirements[65] and refines the security concept of operations to reflect the material solution.[66] Systems security engineering ensures that: (i) protection-relevant aspects of the desired system are captured in the transformation of the stakeholder's requirement-driven view into a technical view; (ii) the functional characteristics of the specified protections are verifiable; and (iii) verification activities are specified to obtain the necessary and sufficient evidence to substantiate assurance claims and to enable a determination of trustworthiness.[67] The system security requirements and security concept of operations provide the basis for the architectural design, implementation, verification, and validation of the system. The security concept of operations is a security-influenced philosophy for the execution and use of the system to protect mission/business processes and assets in a manner that achieves the operational objectives of the organization.

### Systems Security Engineering Outcomes

The following *outcomes* can be expected from the successful execution of a security-enhanced Requirements Analysis Process:

- Security constraints that affect the architectural design of a system and the means to realize it are specified;
- System security requirements that specify the required security characteristics, attributes, functions, and performance for a system solution are defined and documented;

[65] System security requirements are developed with the system requirements. These requirements define the protection capabilities provided by the system, the performance and behavioral characteristics exhibited by the system, and the evidence used to substantiate claims that the system security requirements have been satisfied.

[66] Systems security engineering ensures protection-relevant aspects of the desired system and/or services are captured in the transformation of the stakeholder's requirement-driven view into a technical view. Systems security engineering activities ensure that the functional characteristics of specified protections are verifiable and that activities are specified to obtain relevant and credible evidence to substantiate assurance and to enable determination of trustworthiness.

[67] The production of evidence to determine the *trustworthiness* of a system as part of verification and validation activities can require a substantial investment of human and material resources. Therefore, it is important that any investments in evidence (i.e., resources expended) are commensurate with what is necessary to substantiate developer claims.

- System security requirements are traceable to stakeholder security requirements;
- Security concept of operations is refined to reflect the specified solution;
- The integrity of system security requirements is achieved;
- The basis for verifying that the system security requirements are satisfied is defined;
- The traceability of system security requirements to stakeholder security requirements is achieved; and
- Key stakeholder concurrence is obtained.

### Systems Security Engineering Activities and Tasks

The following security-related *activities* are conducted as part of the Requirements Analysis Process:

- Define system security requirements; and
- Analyze and maintain system security requirements.

#### RA-1: DEFINE SYSTEM SECURITY REQUIREMENTS

RA-1-1: Define the security functional boundary, security domains, trust domains, and context of the system in terms of the security behavior and properties to be provided.

Supplemental Guidance: The security perspective of the system is grounded in the functional boundary of the system and system context. The functional boundary identifies the set of system elements that compose the system-of-interest to be delivered by the engineering effort. The system context consists of: (i) the system-of-interest, boundaries of the system-of-interest, and the environment in which the system-of-interest operates; (ii) other system elements and their associated boundaries and environments of operation; (iii) interconnections between the system-of-interest and other system elements; (iv) services provided by the system-of-interest or provided to the system-of-interest by the other system elements; (v) data and information flows and control flows between the system-of-interest and other system elements; and (vi) assignment of responsibility for implementation of system security requirements individually to the system-of-interest or to other system elements, or jointly by the system-of-interest and other system elements. The security functional boundary may be physical and/or virtual. Security domains and trust domains reflect a security-focused partitioning of the system that group trust relationships between security-enforcing and security-supporting functions. Alternative definitions of the system context are considered to ensure that the system-of-interest can be provided within constraints established by the stakeholders. The system context is defined before refining the security concept of operations and developing the system security requirements. Engineering trade decisions determine and select options for defining the boundaries between the system-of-interest and the system elements with which the system interacts. The boundaries include physical and logical boundaries. Identification of the boundaries determines the interconnections for which trust relationships are required between the system-of-interest and other system elements with which the system-of-interest interacts.

RA-1-2: Define each security function that the system is required to perform and develop the security concept of operations for the intended use of the security functions of the system.

Supplemental Guidance: The security function definition describes how the system protection mechanisms work, individually and collectively. The refined security concept of operations explains how those mechanisms are intended to be used to protect assets while supporting the mission/business. The security function definition results from requirements analysis decisions made to determine the specific protective measures/protections to be incorporated in the system. The security concept of operations provides the security-focused philosophy for how the system protects mission/business assets within the scope of the system concept of operations. The security concept of operations includes the security interconnection and interaction between the system-of-interest and other system elements. Each interconnection and interaction requires identification of interfaces and the data and control flows between the system-of-interest and system elements. The security-relevant properties and attributes of the interfaces, and data and controls flows (e.g., classification or other sensitivity; privacy; and other properties related to confidentiality, integrity, and availability concerns) are identified using the stakeholder security requirements and system concept of operations as input.

System security functions are defined in close coordination with definition of other system functions to ensure cost-effective protections that properly integrate with the system. The protections provided by security functions eliminate or reduce vulnerabilities, or contain impact resulting from the exploitation of vulnerabilities by threats. The security functions also serve to monitor the actions of threat sources and system behavior such that it is possible to predict or detect conditions indicative of threat events that constitute malicious exploitation and non-malicious triggering of vulnerabilities. System security functions also serve to provide for secure configuration, reconfiguration, adaptation, response, and recovery from the impact of threat events, and do so while providing for the protection of assets.

This protection is not necessarily absolute in its effect (e.g., the assets may suffer some degradation, loss of integrity) or comprehensive in its coverage (i.e., all assets may not be protected). Protection needs elicitation includes stakeholder requirements for resilient, secure behavior to avoid, prevent, withstand, and respond to malicious and non-malicious threats and system behavior.

RA-1-3: Define necessary implementation constraints including: (i) constraints that are introduced by the stakeholder requirements or that are unavoidable security solution limitations; and (ii) constraints that are imposed by the system security requirements on the system requirements or that are unavoidable solution limitations imposed by the system security requirements.

Supplemental Guidance: To the extent possible, system security requirements are specified to not constrain a system architectural design and the methods to realize the design. Security-relevant constraints can originate from multiple sources. The Asset Protection Model contains data about system protection functions for mission/business and system assets. This data can be used to identify relevant legal, regulatory, Executive Order, directive, policy, and authorization implications for the system. The engineering team reviews these implications to identify architectural design and implementation constraints for the system. The Asset Protection Model also identifies constraints on the architectural design and implementation of critical functions of the system that derive from mission/business objectives and from system self-protection objectives. The system security requirements are specified across a range that includes a design-independent statement of capability without constraining factors to a design- and/or implementation-dependent statement of capability with specific and perhaps restrictive constraints that limit how all requirements are satisfied. The engineering team analyzes such alternatives to determine the constraints that are necessary for each security function.

RA-1-4: Define technical and quality in use measures that enable the security assessment of technical achievement.

Supplemental Guidance: Each system security requirement may express the functional protection capability or the nonfunctional properties of the protection capability. Each requirement is expressed such that its verification is possible via methods and techniques such as analysis, inspection, measurement, observation, test, evaluation, or other defined and achievable means. Further, the verification methods and techniques produce evidence that contributes to the level of assurance (i.e., confidence) in the protections. These methods and techniques combine to enable a system-holistic assessment that is grounded in a system security perspective sufficient to provide conclusive results. The methods and techniques used to verify each system security requirement are identified and traced to each system security requirement. This traceability includes identifying evidence to be generated to support verification.

RA-1-5: Define system security requirements.

Supplemental Guidance: System security requirements consist of security functional, nonfunctional, and verification /assurance requirements. The term *security functional requirement* is used to distinguish the security requirements that provide a form of protection via behavior (i.e., capability) from the security requirements that provide quality aspects associated with the protection capability. Functional security requirements specify the protection capabilities provided by the system and the capability for secure management of the system. Nonfunctional security requirements address security behavioral, performance, strength-of-function, and quality characteristics and attributes of the system. The assurance requirements identify the techniques and methods employed to generate specific evidence that is used to: (i) provide assurance that the system meets its functional and nonfunctional security requirements; (ii) substantiate the trustworthiness of the system; and (iii) assess the risk associated with the use and operation of the system to support the mission/business.

The system security requirements are developed by performing a requirements analysis of the stakeholder security requirements that includes engineering trade space analyses of alternative means to provide the required protections and to implement risk treatment decisions. The requirements analysis makes use of: (i) relevant regulations, directives, policies, or guidance; (ii) industry best practices and other proven means and methods; and (iii) requirements from similar systems. System security requirements may include or cite standards to which the system must demonstrate compliance. The use of standards-based requirements aids in establishing commonality and interoperability across the functions and services that compose the system and among interconnected systems. Standards-based requirements also

contribute to the trustworthiness of the system by establishing: (i) common behavior of compliant functions and services; (ii) the minimum strength-of-function/mechanism for compliant functions and services; and (iii) test suites to demonstrate compliance in a consistent and repeatable manner.

RA-1-6: Determine the responsibility for system security requirement satisfaction.

Supplemental Guidance: Requirements analysis includes determining responsibility to satisfy the system security requirements. Responsibility may be allocated fully to the system-of-interest or to other system elements, or may be shared by the system-of-interest and other system elements. Stakeholders responsible for system elements that satisfy system security requirements negotiate agreements specifying this responsibility, which includes responsibility for managing the risk associated with the requirements the stakeholders agree to satisfy. These agreements are necessary to ensure the sufficiency, effectiveness, and trustworthiness of end-to-end protections, and to effectively manage the mission/business risk associated with the end-to-end protections when the risk management responsibility is shared. The engineering team identifies and tracks assumptions and other security-relevant information associated with the stakeholder agreements to ensure that the system security requirements and security concept of operation are consistent with the terms of the agreements. The engineering team is not responsible for determining the content of stakeholder agreements. However, it is the engineering team's responsibility to craft a verification strategy that is consistent with the allocated responsibility and that produces verification results that are meaningful and conclusive relative to the agreements between stakeholders.

References: None.

RA-2: ANALYZE AND MAINTAIN SYSTEM SECURITY REQUIREMENTS

RA-2-1: Analyze the integrity and effectiveness of the system security requirements.

Supplemental Guidance: The engineering team analyzes the system security requirements to ensure that individual and combinations of security requirements meet the criteria applied to all requirements (i.e., the requirement is unique, complete, unambiguous, consistent with all other requirements, implementable, and verifiable). The effectiveness of the system security requirements is measured by determining the susceptibility of the system protections specified by those security requirements to threats. The threat susceptibility includes consideration of the security concept of operations. The engineering team uses threat and vulnerability assessment results to determine susceptibility to threats, and to conduct additional threat and vulnerability assessments that are focused on protections specified by the system security requirements as those requirements are decomposed and become more mature in response to the increasingly detailed and refined architectural design.

RA-2-2: Convey the analyzed system security requirements to the applicable stakeholders to ensure that the specified system security requirements adequately reflect the stakeholder security requirements and are sufficient to address their protection needs and protection expectations.

Supplemental Guidance: Providing feedback to stakeholders and obtaining their concurrence is necessary to determine that the results of the requirements analysis process are sufficiently complete and accurate to proceed to architectural design. This includes: (i) explaining to key stakeholders the definition and context for the security of the system and the security concept of operations; (ii) explaining to key stakeholders how the system security requirements meet the stakeholder security requirements, available alternatives, and risks associated with the security requirements and security concept of operation; and (iii) obtaining approval and concurrence from key stakeholders to proceed with developing the architecture for the system. The evidence generated during the requirements analysis demonstrates to key stakeholders the necessity, sufficiency, effectiveness, and completeness of the security requirements in addressing their protection needs. This includes ensuring that key stakeholders understand the decisions that contributed to the definition of the system security requirements and security concept of operations in meeting stakeholder security requirements. The engineering team informs the key stakeholders of the risk associated with the system security requirements and the security concept of operations, allowing them to address and attempt to resolve any concerns before proceeding with development of the system. The engineering team ensures that the appropriate content from the requirements body of evidence is available to support independent verification, validation, and authorization activities associated with the development of the system. Providing stakeholder feedback is not a one-time activity. Rather, this activity is repeated for each iteration/change in the system security requirements.

RA-2-3: Demonstrate traceability between the system security requirements and the stakeholder security requirements.

Supplemental Guidance: The engineering team conducts a traceability analysis for the security concept of operations and system security requirements. This analysis helps to ensure completeness and coverage of the stakeholder security

requirements. Traceability analysis demonstrates that all system security requirements and the security concept of operations have been traced to and are justified by at least one stakeholder security requirement. It also demonstrates that each stakeholder security requirement is satisfied by at least one system security requirement. The engineering team resolves any gaps identified by the traceability analysis to ensure that all stakeholder security requirements are satisfied and that all system security requirements are justified. The engineering team also develops a requirements traceability matrix to capture each system security requirement and trace the requirement to the stakeholder security requirements. The engineering team continually updates the traceability matrix to trace and relate all information associated with the system security requirements as those requirements are decomposed, become more mature, and are refined during architectural design and in subsequent processes.

RA-2-4: Maintain the system security requirements and associated rationale, decisions, and assumptions throughout the system life cycle.

Supplemental Guidance: The engineering team maintains the system security requirements as an integral part of the system requirements baselines. The system security requirements and supporting rationale, decisions, and assumptions include those that specify: (i) functional and nonfunctional aspects of protection capability; and (ii) verification and validation techniques, activities, and tasks and the evidence to be produced by the application of those techniques, activities, and tasks.

References: NIST Special Publication 800-37.

## 3.3 ARCHITECTURAL DESIGN PROCESS

***Purpose***

"The purpose of the *Architectural Design Process* is to synthesize a solution that satisfies system requirements. This process encapsulates and defines areas of solution expressed as a set of separate problems of manageable, conceptual and, ultimately, realizable proportions. It identifies and explores one or more implementation strategies at a level of detail consistent with the system's technical and commercial requirements and risks. From this, an architectural design solution is defined in terms of the requirements for the set of system elements from which the system is configured. The specified design requirements resulting from this process are the basis for verifying the realized system and for devising an assembly and verification strategy."



### Systems Security Engineering Purpose

Systems security engineering, as part of the *Architectural Design Process*: (i) identifies and examines one or more security architectural design and implementation strategies; and (ii) identifies, minimizes, and contains the impact of vulnerabilities, taking into account susceptibility to threats and stakeholder risk tolerance. A security architectural design solution that provides a sufficient level of trustworthiness is defined in terms of the security requirements for the security-relevant system elements. The protections specified by the security design requirements are iteratively refined into security specifications and security procedures from which the system is implemented, configured, operated, and maintained.

### Systems Security Engineering Outcomes

The following *outcomes* can be expected from the successful execution of a security-enhanced Architectural Design Process:

- The system security architectural design baseline is established;
- An implementable set of system security elements is specified;
- Security interface requirements are incorporated into the architectural design solution;
- Security architectural design is traceable to the system architectural design and to the system security requirements;
- Procedural security measures are established;
- A basis for verifying the security-relevant system elements and end-to-end protection capabilities is defined;
- A basis for secure integration of system elements is established;
- An architecture risk assessment is conducted; and
- Key stakeholder concurrence is obtained.

### Systems Security Engineering Activities and Tasks

The following security-related *activities* are conducted as part of the Architectural Design Process:

- Define the security architecture;
- Analyze and evaluate the security architecture; and
- Document and maintain the security architecture.

AD-1: DEFINE THE SECURITY ARCHITECTURE

AD-1-1: Define the logical security architectural design.

Supplemental Guidance: Security architectural design is developed with the system architectural design and considers the mission/business, operational concepts, stakeholder requirements, system requirements, priorities, cost, schedule, performance, threat, vulnerability, and risk. The security architectural design includes assessing trade-offs between the relative strengths and weaknesses of each design option to achieve an optimal cost/benefit balance between the system life cycle protection capability provided and the risk. The security architecture contributes properties that provide or that enable security capability: (i) to protect mission/business assets; (ii) to protect system assets; and (iii) for security management to effectively configure, operate, and sustain the system across specified normal and degraded operational and sustainment modes. System properties derived from security architectural design also contribute to the achievement of operational resiliency of system functions/services in response to the impact of physical and cyber attacks, human errors, component faults and failures, and disaster events.

The security architectural design is developed by: (i) application of architectural protection strategies, methods, tools, techniques, and technologies; (ii) the application of trust principles and concepts; and (iii) adherence to reference security architectures and associated methods. Architectural design and trust principles and concepts include, but are not limited to, separation, isolation, encapsulation, non-bypassability, layering, modularity, hierarchical trust, hierarchical protection, and secure distributed composition. The security architectural design puts emphasis on the interconnections and interactions that provide end-to-end protection for business/mission processes and the provision of services. Security architectural design concepts apply beyond the system architecture to include infrastructure and service model abstractions for the provision of services. Examples of architectural, infrastructure, and service model abstractions include layered, centralized, distributed, client-server, multitiered, service-oriented, and cloud. Each of these presents their own considerations, constraints, advantages, and disadvantages relative to security architectural design.

AD-1-2: Partition the system security functions identified in requirements analysis, allocate those functions to elements of the system security architecture to achieve trust relationships, and generate derived security requirements as needed for the allocations.

Supplemental Guidance: The engineering team: (i) determines the security-relevant elements of the system; (ii) allocates system security requirements to the security-relevant elements; (iii) places the elements in the system architecture; (iv) defines and describes the trust relationships between the security-relevant elements; and (v) provides a security-focused narrative about the system security architecture and its security properties that is sufficient to guide the design and implementation of the system. The placement of security-relevant functions and definition of trust relationships applies security principles/concepts as well as best practices such as defense-in-depth and defense-in-breadth. The placement of security-relevant functions includes consideration of architecture, infrastructure, and service models employed or to be employed by the system, and the concept of operations for mission/business processes.

The allocation of system security requirements defines what, if any, security-relevant responsibility is assigned to each system element. The allocation of system security requirements is to be compatible with the infrastructures and services reflected in the architectural design. The allocation provides protection for the stakeholder/system data, information, and capability assets. The Asset Protection Model and existing architecture information (i.e., the enterprise architecture, security architecture, or other guiding organizational architectural artifacts) inform the security partitioning and security functional allocation. The allocation is to be consistent with the security concept of operations for interaction with: (i) other security processes, functions, and services; (ii) non-security-relevant processes, functions and services; and (iii) the environment of operation.

The system security requirements to be satisfied by technical means are implemented within end-point user computing platforms and within the computing platforms located within the network infrastructure of the system. End-point computing platforms can be stationary or mobile user-accessible devices such as workstations, desktops, laptops, or hand-held devices. The system security requirements to be satisfied by physical safeguards and procedural measures performed by individuals are allocated to be mutually supportive of the system security requirements satisfied by technical means. The engineering team determines the relationships and dependencies between the security-relevant system elements and supporting physical safeguards and procedural measures. These relationships and dependencies are documented to demonstrate how they combine to satisfy the system security requirements.

Considerations that impact the functional allocation include:

- Whether technical, physical, or procedural measures, alone or in combination, are most appropriate to implement the system security requirements;
- Whether acquiring an off-the-shelf product, accessing or subscribing/leasing a service, or custom software development or hardware fabrication is most appropriate to implement the system security requirements;
- Which options are appropriate to resolve issues that surface during refinement of the design; and
- Whether the selection of a product or service will be made during this phase or postponed to the implementation phase.

The engineering team identifies additional security requirements resulting from architectural decisions made during this process and ensures that those requirements are incorporated into the requirements baseline. Additional requirements are categorized as either being derived from existing requirements or constituting new system security requirements. Derived system security requirements refine and/or extend the system security requirements baseline developed in the previous process. Each derived system security requirement is traceable to at least one system security requirement. The identification of new and derived requirements indicates that stakeholder security requirements and security design requirements must be revisited, as needed, to ensure consistency and traceability between the architectural design and all requirements baselines. This further requires that the Stakeholder Requirements Definition (SR) process and the Requirements Analysis (RA) process are iteratively and recursively performed in conjunction with the decisions made during this process.

AD-1-3: Define and document the security interfaces, security interconnections, and the trust relationships between system elements and between the system and external systems.

Supplemental Guidance: Trust relationships between interconnected components are the building blocks for a secure system, and the basis for composing end-to-end protection. The security architecture provides the view of the system architecture that depicts: (i) how security-relevant functions are allocated to individual system elements (making those elements *trusted* system elements after appropriate assurance arguments are made); (ii) the trust relationships between the trusted system elements; (iii) the information flows and interconnections that realize the trust relationships; and (iv) how the trusted system elements combine and interact with each other and with the other parts of the system to deliver the specified protection capability. Security architecture provides the basis for understanding: (i) the different levels of trust within the system; (ii) where the levels of trust exist; (iii) the information flows that occur within a level of trust; and (iv) the information flows that cross trust-level boundaries. This understanding informs the allocation of functional/assurance requirements to security-relevant system elements, and provides the basis for engineering trade decisions and security risk management. With a high-level security architectural understanding in place, focus is subsequently directed at the internals of the security-relevant system elements, applying these same security-relevant, trust, and trust relationship concepts in smaller contexts to successively decompose the system into its primitive components. This iterative decomposition and understanding of the system builds confidence through the accumulation of evidence about the internals of individual system elements, how they combine to form composite system elements, and how the composite system elements combine to form the system.

References: None.

### AD-2: ANALYZE AND EVALUATE THE SECURITY ARCHITECTURE

AD-2-1: Analyze the resulting security architectural design to establish security design criteria for each element.

Supplemental Guidance: Design criteria are provided in specifications for technology elements and for physical system elements, and in policies and procedures that govern the behavior and actions of individuals for direct interaction with and support to the system. The system element specification and policies and procedural are developed with detail that is sufficient to proceed with implementation of the design—that is, until there all no further design decisions to be made. The operational security policies and procedures are designed to complement technical and physical elements by ensuring that the security-relevant activities of individuals are defined and described. The scope of the security policies includes: (i) establishing and maintaining an appropriate environment in which the elements can be installed and operated properly using the security functions of the elements in support of the mission/business; (ii) determining authorization for users to access and use the system and information; and (iii) ensuring that security-relevant life cycle concerns are addressed throughout the life cycle of the system. Proper use has a scope that includes the entire life cycle of the solution and applies to all individuals that have reason to interact with the system.

AD-2-2: Determine which system security requirements are allocated to authorized operators, maintainers, administrators, and other designated authorized users.

Supplemental Guidance: Task AD-1-2 allocated security functions to the system security architecture. Part of that allocation is the determination of those functions performed by individuals. Defining authorized individuals and allocating well-defined security responsibilities to those individuals is necessary to achieve a trustworthy system. The system security requirements to be satisfied by physical safeguards and procedural measures are allocated to the authorized operators, administrators, and users so those requirements are mutually supportive of the system security requirements satisfied by technical means. The engineering team determines the relationships and dependencies between the security-relevant system elements and supporting physical safeguards and procedural measures. These relationships and dependencies are subsequently documented to demonstrate how they combine to satisfy the system security requirements. The engineering team reviews the security concept of operations and security functional allocation to allocate security requirements (i.e., responsibility for satisfying those requirements) to system operators, administrators, and users, based on the defined roles and responsibilities. The trustworthiness of individuals serving in designated authorized roles is also addressed in the determination of which system security requirements are satisfied by individuals. The trustworthiness of individuals must be equivalent to that of the system security function that they perform or support.

AD-2-3: Determine whether existing infrastructures, services, and hardware/software elements that satisfy the security architectural design and interface criteria are available.

Supplemental Guidance: The engineering team considers cost-effective alternatives to custom hardware fabrication and custom software development. This applies to all system elements and includes security-relevant system elements. Life cycle security considerations are also a factor in selecting among viable options. For security-relevant system elements, security functional and assurance requirements, security risk, and life cycle support are considered. Gaps between the security functional requirements and that which is actually provided are considered. Note that the consideration can include two different cases: (i) the candidate system element that is obtained provides less than the specified security requirements (i.e., a deficiency in functionality or assurance); and (ii) the candidate system element that is obtained provides a capability beyond that specified (i.e., additional functionality that cannot be verified and that can potentially cause unwanted security-related side effects).

AD-2-4: Evaluate alternative security architectural design solutions, modelling those solutions to a level of detail that permits comparison against the specifications expressed in the system security requirements and the assurance and trustworthiness, risk, performance, cost, and time scales expressed in the stakeholder security requirements.

Supplemental Guidance: The engineering team analyzes and evaluates alternative architectural designs and associated engineering trades and risk treatment trades to assist in system architectural and element design. The team selects among alternative reference security architectures and other proven architecture forms and models. To do so, the team (i) determines the strengths and weaknesses of candidate architectures; (ii) considers constraints such as mandated compliance and interaction with existing systems, services, and infrastructures, and the mandated reuse or adaptation of elements of existing systems, services, or infrastructures; and (iii) considers constraints on the scope and type of changes that can be made to the solution architecture and to the concept of operations. The analysis of the security architectural design focuses on security-enforcing, security-supporting, and security non-interfering functions. The engineering team determines: (i) if the system security architecture is compliant with the system security requirements and the security concept of operations; and (ii) if the security architecture provides a suitable framework for the design of the security-relevant system elements. The engineering team conducts a traceability analysis to ensure completeness and coverage in the allocation of system security requirements to system elements in the system security architecture and to the physical safeguards and the procedural measures in the environment of operation. The system security architecture and the functional allocation of requirements are also traced back to the security concept of operations and system security requirements. This traceability analysis helps to ensure that: (i) each system element, physical safeguard, and procedural measure is justified by satisfying or contributing to satisfying a system security requirement; (ii) all system security requirements are satisfied; and (iii) the system security architecture and supporting physical safeguards and procedural measures provide a sufficient basis for the design of the system. The engineering team documents decisions that result from security architectural design decisions.

The engineering team determines the security-relevant merits, limitations, and risks associated with candidate design options. The engineering team considers security-influenced recommendations when selecting among candidate options and ensures that security-relevant life cycle information and considerations are provided and are suitable to influence selection among available options. Design trade-off analyses consider mission/business operations, operational concepts, stakeholder requirements, priorities, cost, schedule, performance, and risk, and other factors identified as critical to stakeholders. Design trade-offs also consider the best approach to satisfying security requirements:

- Whether technical, physical, or procedural measures, alone or in combination, are most appropriate to implement the system security requirements;
- Whether acquiring an off-the-shelf product, accessing or developing a service, or custom development is most appropriate to implement the system security requirements;
- Which options are appropriate to resolve issues that surface during refinement of the design;
- Whether the selection of a product or service is made during this process or postponed to the implementation process; and
- Whether the architectural approach meets the system security requirements (i.e., does the architecture contain provisions for high availability [if required], does the architecture allow for all required data flows as identified in the Asset Protection Model).

As the system architectural design is successively decomposed into major and minor system subsystems and components, security analyses are conducted to ensure that element security specifications achieve an acceptable balance across existing and new constraints. Element security design analyses verify that all aspects of each element design are necessary to meet its allocated security requirements. The security design analyses also determine that the design for combinations of elements and for trust relationships between elements properly contribute to meeting the allocated system security requirements and do not introduce unspecified capabilities. These analyses help to ensure that the system design is not over-engineered or under-engineered. An over-engineered design reflects requirements creep. It possesses protection capability or strength of function/mechanism that is not necessary or that is excessive, relative to the solution security requirements. An under-engineered design provides inadequate protection capability or strength of function/mechanism. Identification of such gaps during this phase reduces cost, should the gaps not be identified until implementation, integration, or during operational use of the solution.

Architectural design trade-off analyses may be repeated many times and at many design abstraction levels before selecting among the options. The trade-off analysis results are formally documented. At a minimum, the documentation includes: (i) the criteria used to conduct the analysis and to assess and select among alternatives; (ii) the decisions that resulted from the analysis; and (iii) the supporting rationale, constraints, and assumptions. Architectural design trade-off analyses include protection needs, threat assessments, and vulnerability assessments to aid in iterative refinement and assessment of the architectural design options. Architectural design risk assessments provide information for comparative assessment of the architectural designs in terms of mission/business risk, and inform the identification of risk treatments. Architectural trade decisions may result in new, changed, deleted, and derived requirements and constraints. These changes require that the Architectural Design Process be repeated in conjunction with iterations of the Stakeholder Requirements Definition Process and the Requirements Analysis Process.

The engineering team also conducts cost-benefit analyses of the security design. The benefit derived from the security design is determined by: (i) the effectiveness of a security function in providing the protection allocated to it; (ii) the trustworthiness that can be placed on the function; and (iii) the risk associated with the use of the function. It is possible that the optimal cost and benefit are realized from the employment of a combination of less costly security functions rather than employment of a single cost-prohibitive function. It may also be the case that a security function may adversely impact the system performance and therefore, preclude the use of such function. The engineering team may consider alternate designs that can meet the stated performance and protection needs or provide an acceptable balance between meeting performance needs while providing protection and remaining within the agreed-upon risk tolerance. Protection needs, threat, vulnerability, and risk assessment outcomes provide information that is used to support cost-benefit assessments of the security design.

The architectural security design has inherent risk. The design may introduce new vulnerabilities or may expose vulnerabilities that would not otherwise be exposed. The employment of security functions in the system architecture can reduce risk in one context while increasing risk in some other context. The cost of the security design and the security functions allocated within the system architecture includes: (i) the cost to acquire/develop, integrate, operate, and sustain the functions over the system life cycle; (ii) the impact to system performance; and (iii) the cost to obtain evidence of assurance sufficient to make a trustworthiness determination.

The analysis of the security architecture includes identification of vulnerability and a determination of the susceptibility to threat given identified vulnerabilities. Existing threat and vulnerability assessment results assist in this analysis; however, it is important to conduct a vulnerability assessment based on security principles and concepts to complement and inform the analyses that are driven by threat. Revisions to the security architectural design and system architectural design eliminate vulnerabilities or reduce or constrain the impact of exploiting/triggering identified vulnerabilities. An architecture risk assessment is conducted to identify risks associated with the architectural design and to determine if those risks exceed risk tolerance. Risks relative to architectural trade-off decisions are captured to support subsequent risk assessment activities and to demonstrate coverage and completeness in addressing risks.

References: None.

AD-3: DOCUMENT AND MAINTAIN THE SECURITY ARCHITECTURE

AD-3-1: Specify the selected physical security design solution as a security architectural design baseline in terms of its functions, performance, behavior, interfaces, interconnections, trust relationships, security domains, and unavoidable implementation constraints.

Supplemental Guidance: The engineering team: (i) develops specifications for the security services, functions, and mechanisms to be implemented within the system security architecture; (ii) develops specifications for physical elements placed in the environment of operation of the system; and (iii) identifies security procedures to operate, manage, and maintain the system. Element specifications describe the capability and behavior of the functions, mechanisms, and services provided by each element, including capability and behavior when interacting via its interfaces with the services and functions provided by other elements. Element specifications include consideration of applicable non-security requirements including, for example: policy; interaction with the physical environment and users; size, weight, and power constraints; performance; and safety. The element specifications are compliant with the constraints imposed by the system security architecture and any interoperability constraints imposed by the portions of the system that cannot be changed. The element specifications leverage design patterns, best practices, and standards to manage risk in the use of technology in system elements, the integration and interoperability of system elements, and the assurance and strength-of-function/mechanism of system elements.

The content of each element specification is determined by the implementation strategy for the element. The detail in the specification is sufficient to allow for implementation without the need for any further design decisions to be made. For system element functions that are developed or fabricated, the specification may also define configuration settings or may dictate or limit implementation decisions (i.e., the manner in which a system security requirement is satisfied). For elements that are obtained as a service or through purchase of an off-the-shelf product, the specification may cite one or more specific services or products as candidates for use in the system.

The verification requirements for accumulation of a body of assurance evidence to support the verification of the design and its implementation are refined and extended with information obtained in performing architectural design activities performed and rationale for engineering trades.

AD-3-2: Record the security architectural design information.

Supplemental Guidance: The engineering team records depictions of the security architectural design and supporting information to describe the security architectural design and to relate it to the system design.

AD-3-3: Maintain mutual traceability between specified design and system requirements.

Supplemental Guidance: Traceability between the security design and the specified design and system requirements demonstrates that the design for each security-relevant system element traces back to one or more system security requirements. It also demonstrates that each system security requirement is satisfied by one or more security-relevant system elements. Security architectural design decisions, engineering trade decisions, and risk treatment decisions result in new, changed, deleted, and derived requirements and constraints. These changes require that the Architectural Design Process be repeated in conjunction with iterations of the Stakeholder Requirements Definition Process and the Requirements Analysis Process. A traceability analysis of the security architecture back to the system security and stakeholder security requirements ensures that all system security requirements are allocated to security-relevant system elements, physical elements, and procedural measures performed by individuals, and that the security architecture is consistent with the system architecture, system security requirements, and security concept of operations.

References: None.

## 3.4 IMPLEMENTATION PROCESS

***Purpose***

"The purpose of the *Implementation Process* is to realize a specified system element. This process transforms specified behavior, interfaces and implementation constraints into fabrication actions that create a system element according to the practices of the selected implementation technology. The system element is constructed or adapted by processing the materials and/or information appropriate to the selected implementation technology and by employing appropriate technical specialties or disciplines. This process results in a system element that satisfies specified design requirements through verification and stakeholder requirements through validation."



*Systems Security Engineering Purpose*

Systems security engineering, as part of the *Implementation Process*, realizes a security-relevant system element and transforms the specified behavior, interfaces, and implementation constraints into secure fabrication, development, and adaption actions. The resultant system element satisfies the security architectural design requirements through security-focused verification and satisfies stakeholder security requirements through security-focused validation.

Systems Security Engineering Outcomes

The following *outcomes* can be expected from the successful execution of a security-enhanced Implementation Process:

- A strategy for secure implementation is defined;
- Security-driven implementation (technology) constraints on the system design and on the security architectural design are identified;
- A security-relevant system element is produced; and
- A system element is packaged and stored according to stated protection measures and agreements for its supply.

Systems Security Engineering Activities and Tasks

The following security-related *activities* are conducted as part of the Implementation Process:

- Plan the security implementation of system elements; and
- Perform security implementation of system elements.

IP-1: PLAN THE SECURITY IMPLEMENTATION OF SYSTEM ELEMENTS

IP-1-1: Generate a security implementation strategy for system elements.

Supplemental Guidance: The strategy for security implementation applies to all system elements regardless of their security-relevant role in the system. The strategy includes procedures and techniques that establish and maintain assurance and trust: (i) in development, adaptation, fabrication, and supply processes; (ii) in the use of supporting tools, equipment, techniques, and methods used by those processes; and (iii) to address security verification uncertainties. System elements with security-relevant roles may require specific trust-driven process enhancements. The secure implementation strategy addresses trusted development methodologies and security authorization for personnel

performing high-confidence and trusted development processes. All system elements present some level of security concerns tied to logistics, supply, and the distribution of components used to implement the design. The strategy for secure implementation addresses and accounts for these concerns.

IP-1-2: Identify security constraints that the security implementation strategy and security implementation technology impose on security and non-security design solutions.

Supplemental Guidance: Security-driven constraints can impact aspects of security design and aspects of non-security design. The engineering team ensures that the security-related constraints affecting all forms and contexts of design solutions, and the associated implications of such constraints, are used to inform requirements elicitation, requirements analysis, architectural design, system concept of operations, and associated procedures (including security policy and procedures).

References: None.

IP-2: PERFORM SECURITY IMPLEMENTATION OF SYSTEM ELEMENTS

IP-2-1: Realize or adapt system elements using the implementation-enabling systems and specified materials according to the defined security implementation procedures.

Supplemental Guidance: Security implementation addresses all aspects of hardware fabrication, software development, adaptation and reuse of existing capabilities, and the acquiring or leasing of components and services, supply chain of system components, and training. The system design is implemented by: (i) obtaining products and services that satisfy the security specifications for system elements to be purchased or leased; (ii) custom development of software and firmware that satisfy security design specifications; (iii) fabricating hardware devices and mechanisms that satisfy security design specifications; (iv) obtaining physical devices and mechanisms that satisfy physical countermeasure specifications; and (v) developing operational policies and procedures to govern the actions of individuals in their use of the system and in support of the security of the system throughout its life cycle. Certain portions of the system may be implemented using a combination of obtained products/services, custom-developed software, or custom-fabricated hardware. These portions of the system are subject to the appropriate development and fabrication processes to ensure that security concerns are identified, resolved, and documented in the same manner as all custom-developed or fabricated portions of the system. Examples include custom-developed interface software or wrappers for obtained products and services required to provide interoperability between interacting system elements of the solution. Custom hardware may be required to satisfy performance constraints. In addition to hardware fabrication and software development, implementation includes policies and procedures addressing operations, maintenance, disposal, training, and the security- relevant aspects of other solution-specific objectives required to support the mission/business.

The selection of products/services obtained by purchase, lease, loan, or contract is based on a variety of factors and selection criteria the majority of which are not security-relevant. The engineering team ensures that security is included in these factors and selection criteria. Concerns include cost, availability, size, weight, power, interoperability, and scalability. Trade studies are typically conducted to select among candidates. These studies include security-relevant factors in the selection criteria and when making decisions. The engineering team determines the merit of each candidate product or service in meeting relevant system element security specifications and the ability of the product or service to support the mission/business. The team employs the product/service merit results as part of the selection criteria. The engineering team analyzes the product and service selection criteria to ensure that all security-relevant concerns are addressed in accordance with defined specifications.

System elements implemented by custom software development and hardware fabrication provide the opportunity to acquire insight to the details of design and implementation including software development and hardware fabrication processes followed. Insight into design and implementation details, decisions, and rationale can increase assurance and trustworthiness in system elements and reduce risk. The engineering team conducts reviews during these activities to identify and resolve vulnerabilities and other security-relevant concerns that would otherwise go unnoticed. Special attention is given to programming and implementation details associated with boundary conditions, input parameters, common vulnerabilities and weaknesses, and exception handling/response to ensure that the behavior of the functions provided by the hardware and software elements are not bypassed, diminished, or altered. While these measures can increase the trust in the design of the software or hardware, the engineering team also considers the exposure of these system elements to other threats. The implementation of additional protection measures addressing personnel security, configuration management, and integrity protection, helps to preserve the level of trust gained from design assurance measures.

IP-2-2: Record evidence that the system elements meet the security aspects of supplier agreements, legislation, and organizational policy.

Supplemental Guidance: The evidence recorded is used to substantiate claims that the security architectural design has been fulfilled by the implemented system element. The engineering team identifies, obtains, correlates, and records all security evidence generated during the implementation of system elements.

IP-2-3: Securely package, store, and distribute the system elements.

Supplemental Guidance: Secure packaging, storing, and distribution of system elements is accomplished in accordance with the secure implementation strategy. This strategy addresses supply, logistics, and provisioning of system elements, and includes adherence to system security requirements, processes, and procedures that establish minimum strength of protections (for both functions and mechanisms) and the conduct of associated processes to preserve the confidentiality, integrity, and availability properties of system elements.

References: None.

## 3.5 INTEGRATION PROCESS

***Purpose***

"The purpose of the Integration Process is to assemble a system that is consistent with the architectural design. This process combines system elements to form complete or partial system configurations in order to create a product specified in the system requirements."



*Systems Security Engineering Purpose*

Systems security engineering, as part of the *Integration Process*, assembles a system that is consistent with the security architectural design. Systems security engineering combines system elements to form complete or partial trusted system configurations to create the security product specified in the system security requirements.

Systems Security Engineering Outcomes

The following *outcomes* can be expected from the successful execution of a security-enhanced Integration Process:

- A strategy for security integration is defined;
- Unavoidable security-driven constraints of integration that influence architectural design are defined;
- A system capable of being verified against the specified security requirements from the security architectural design is assembled and integrated; and
- Security nonconformances to security requirements due to integration actions are recorded.

Systems Security Engineering Activities and Tasks

The following security-related *activities* are conducted as part of the Integration Process:

- Plan for security integration of system elements; and
- Perform security integration of system elements.

IN-1: PLAN THE SECURITY INTEGRATION OF SYSTEM ELEMENTS

IN-1-1: Define an assembly sequence and strategy that minimizes system security integration time, costs, and risks.

Supplemental Guidance: The security integration strategy composes increasingly larger and more complex system elements and configuration (e.g., component subsystems, system subsystems) until the entire system-of-interest is realized. The security integration strategy focuses on trust relationships and ensuring that proper attention is given to the manner in which end-to-end system protections are composed from the constituent security elements. The strategy is tied to verification and validation activities to preserve the individual component assurances and to compose trusted system-level protections across the hardware and software, physical, and procedural system elements. This includes limiting the pace at which security integration occurs to ensure that evidence can be generated given the availability of system components, enabling systems, subsystems, test suites, simulators, and test data.

IN-1-2: Identify the security constraints on the architectural design resulting from the system integration strategy.

Supplemental Guidance: Trusted end-to-end security protections are realized by the interconnections and interfaces of security-relevant system elements. Security-driven constraints associated with system element integration and assembly may limit or dictate system and security architectural design trade space options and decisions.

References: None.

IN-2: PERFORM SECURITY INTEGRATION OF SYSTEM ELEMENTS

IN-2-1: Obtain integration-enabling systems and specified materials according to the defined system integration procedures.

Supplemental Guidance: The engineering team ensures that the integration-enabling systems obtained to provide support for security integration comply with the defined integration procedures.

IN-2-2: Obtain system elements in accordance with secure distribution considerations, requirements, and constraints documented in agreements.

Supplemental Guidance: The handling, storage, distribution, delivery, and acceptance of system elements is to be accomplished to comply with agreements and in a manner that preserves the confidentiality and integrity attributes defined for the system elements.

IN-2-3: Assure that the security-relevant system elements have been verified and validated against security acceptance criteria specified in an agreement.

Supplemental Guidance: Integration cannot be completed until all security verification and security validation criteria are satisfactorily met. Verification is intended to demonstrate that the system was built correctly in accordance with the specified system security requirements and security architectural design. Validation is intended to demonstrate that the right system was built in accordance with stakeholder protection needs, and that the system is sufficiently trustworthy to be relied upon to properly enforce organizational security policies and protect stakeholder's assets. See *Verification* and *Validation* Processes.

IN-2-4: Integrate security-relevant systems elements in accordance with applicable interface control descriptions and defined assembly procedures, using the specified integration facilities.

Supplemental Guidance: Security integration serves to compose the specified end-to-end protection capability. It does this by realizing the trust relationships that exist between security-enforcing and security-supporting system elements. Security integration occurs in the context of security and trust domains. The security architectural design identifies these domains and provides the framework for security integration. Further, each security and trust domain has a management function that has its own interconnections, interfaces, and interface control descriptions.

IN-2-5: Analyze, record, and report security integration information, including results of security integration actions, nonconformance, and corrective actions taken.

Supplemental Guidance: The engineering team defines security configuration settings and information. These settings and information support engineering team verification and validation activities as well as the independent verification and validation activities conducted by various stakeholders. The settings and information also support operational and maintenance procedures, and provide the basis for training materials. Changes to security configurations are recorded and approved following established configuration management procedures. The engineering team records/reports: (i) data on system performance and unanticipated system behavior and factors encountered; ii) evidence to support assurance and trustworthiness claims associated with security-relevant system elements and the overall system; (iii) security integration nonconformance, and (iv) resolution to security integration nonconformances and corrective active for security integration.

References: None.

## 3.6 VERIFICATION PROCESS

***Purpose***

"The purpose of the *Verification Process* is to confirm that the specified design requirements are fulfilled by the system. This process provides the information required to effect the remedial actions that correct nonconformances in the realized system or the processes that act on it."



*Systems Security Engineering Purpose*

Systems security engineering, as part of the *Verification Process*, demonstrates that the system was built *correctly*. In particular, security verification demonstrates that implemented protective measures: (i) satisfy stakeholder security requirements and the security architectural design; (ii) exhibit no unspecified behavior; (iii) provide continuous protection in all defined system modes of operation; (iv) are resistant to attack and misuse; and (v) satisfy the trustworthiness objectives of stakeholders. Additionally, security verification identifies vulnerabilities and determines how those vulnerabilities may be exploited or triggered, thereby determining the susceptibility to threat.

Systems Security Engineering Outcomes

The following *outcomes* can be expected from the successful execution of a security-enhanced Verification Process:

- A strategy for security verification is defined;
- Security verification constraints on system design requirements and architectural design are defined;
- Information for security-relevant corrective actions is reported; and
- Sufficient evidence is provided to substantiate that the realized product:
  - Satisfies the system security requirements;
  - Satisfies the security architectural design;
  - Provides continuous protection in all defined modes of system operation;
  - Is sufficiently resistant to attack and misuse; and
  - Satisfies the trustworthiness objectives of stakeholders.

Systems Security Engineering Activities and Tasks

The following security-related *activities* are conducted as part of the Verification Process:

- Plan the security verification of the system; and
- Perform security verification of the system.

VE-1: PLAN THE SECURITY VERIFICATION OF THE SYSTEM

VE-1-1: Define the strategy for system life cycle verification of security-relevant system elements and system security.

Supplemental Guidance: The security verification strategy applies to all forms of system description (concept of operation, security requirements, security architectural design). The security verification strategy includes the context and purpose of each instance of a verification action (e.g., verifying the security requirements; verifying the security architectural design, the ability to implement the security design correctly, the ability to detect, resist, and react to attacks, errors, failures, or misuse, and the ability to predict errors, and failures). The security verification method (inspection, demonstration, test, analysis, or a combination therein) is determined for each verification action. The depth, breadth, and rigor of verification actions is a function of the degree of assurance (confidence) desired to substantiate trustworthiness claims and to inform risk assessment and risk treatment decisions. The strategy also includes an implementation and use case-directed vulnerability assessment which scopes penetration/misuse testing to identify the means and methods used to exploit vulnerabilities via intentional attacks or to trigger vulnerabilities via incidental and accidental actions.

VE-1-2: Prepare a security verification plan based on system security requirements and assurance objectives.

Supplemental Guidance: Security verification plans account for the various configurations and operational modes defined in the security integration strategy. The security verification activities in the plan: (i) progressively build assurance; (ii) provide a basis for determining the trustworthiness of the fully configured product; and (iii) inform risk assessment and risk treatment decisions.

VE-1-3: Identify constraints on system and security design decisions that result from the security verification strategy and plan.

Supplemental Guidance: Security verification limitations, practicalities, and uncertainty may limit the conduct of verification or the assurance that can be achieved by verification. Such constraints are used to inform the security architectural design trades decisions, to include decisions associated with options to realize a security-relevant system element (i.e., to fabricate, develop, reuse, adapt, purchase, or lease).

References: None.

VE-2: PERFORM SECURITY VERIFICATION OF THE SYSTEM

VE-2-1: Ensure that the enabling systems, test suites, equipment, simulators, facilities, and operators used for security verification are available and prepared for the verification of security-relevant system elements.

Supplemental Guidance: Security verification activities may require specialized tools and the application of certain techniques that require specialized expertise and skills.

VE-2-2: Conduct security verification to demonstrate that: (i) system security requirements and security architectural design are satisfied; (ii) security protections are continuous in all defined modes of system operation; (iii) the system is sufficiently resistant to attack and misuse; and (iv) sufficient evidence exists to demonstrate achievement of trustworthiness objectives.

Supplemental Guidance: Security verification is conducted at various levels (e.g., mechanism, function, component, service, subsystem, system, and system-of-systems) and includes technical, physical, and procedural elements of the system, as well as all supporting life cycle processes for development, supply chain, operations, and sustainment of the system. Security verification is conducted on individual system elements and on combinations of elements, typically based on the partitioning and trust relationships expressed in the security architectural design of the system, and in terms of system elements and how those elements interact within the system. Additionally, security verification continuously builds the evidence required to substantiate claims of correctness, quality, performance, and strength-of-mechanism from the perspective of satisfying protection needs and enforcement of security policy within the broader capability and performance constraints of the system. Security verification is conducted in accordance with a specific verification strategy put in place during requirements elicitation and analysis, and is updated as the design matures and supports operations. Corrective actions are initiated as appropriate to resolve demonstrated noncompliance. Security verification is undertaken in a manner consistent with organizational constraints, such that uncertainty in the replication of security verification actions, conditions and outcomes is minimized. Security verification actions and outcomes are documented and approved.

The integrated security elements of the system are verified to determine that the elements meet the system security requirements. Element configurations are verified to ensure they meet design specifications. Element configuration is determined to ensure that the required security services and security functions are enabled, provide the required level of protection and strength of function/mechanism, and interoperate with other security-relevant and nonsecurity-relevant services and functions in the system. Any unused or unnecessary system functions constitute risk that can be reduced or prevented. Therefore, those functions are preferably removed from the system or disabled. If removal or disabling of the functions is not possible, the functions are configured to restrict access to a limited set of users who are aware of their existence and associated vulnerabilities. If it is not possible to prevent or limit the use of the extraneous functions and features, recommendations for appropriate procedural protections are provided.

VE-2-3: Conduct a vulnerability assessment to identify exploitable vulnerabilities and vulnerabilities that may be triggered by errors of omission, commission, or by component faults and failures.

Supplemental Guidance: The vulnerability assessment is conducted as a comprehensive activity that identifies all types of weaknesses that can be intentionally exploited and that can be unintentionally triggered. The objective of the vulnerability assessment is to identify weaknesses in: (i) system functions; (ii) system designs; (iii) acquired products and services; (iv) developed capability and technology; (v) engineering documentation; (vi) manufacturing, development, fabrication, operations, maintenance, logistics and supply chain processes; and (vii) all associated tools, techniques, and procedures. The vulnerability assessment includes reviews, inspections, and analyses of the system concept of operations, requirements, security policy, security architectural design, data and information flow, and development, design, supply chain/logistics, and sustainment processes.

The focus and objectives of the vulnerability assessment change as the system moves through the development stages of the system life cycle and into the operations and sustainment stages. Early in the system life cycle, the vulnerability assessments typically focus on security policy objectives, requirements, architecture, and high-level designs. As the system design matures and the system is placed into operation, there is greater insight to existing vulnerabilities, identification of new vulnerabilities, and an increased understanding of how multiple vulnerabilities may relate and interact. An additional form of vulnerability assessment is conducted during implementation, integration, and once the system is put into operational use and undergoes sustainment. This form of vulnerability assessment focuses on determining the effectiveness of the protective measures and on identifying opportunities to defeat those measures. The vulnerability assessment proactively seeks to determine how protective measures might be misused, mismanaged, attacked, or incorrectly configured. And finally, vulnerability assessment supplements fault diagnosis to a level of resolution consistent with cost effective remedial action, including re-verification following defect correction, and/or organizational quality improvement actions.

VE-2-4: Conduct penetration testing to identify methods by which vulnerabilities may be intentionally exploited or unintentionally triggered.

Supplemental Guidance: Penetration testing is a type of verification activity specific to security. Penetration testing is a strategized, planned, and controlled attempt that is intended to breach the protective measures implemented within the system. The penetration test simulates the actions of a given class of attacker within the context of specific *rules of engagement* by using the knowledge, methods, techniques, and hardware and software tools the attacker is expected to employ to attempt to circumvent the security protections of a system. Penetration testing results provide information about the system that supplements the information that can be obtained through all other security verification methods. The information obtained from penetration testing results provides insights that: (i) enhance the engineering team's understanding of the system; (ii) uncover weaknesses or deficiencies in the system; and (iii) indicate the level of effort required on the part of adversaries to breach the security measures implemented in the system. Consideration is given to performing penetration tests: (i) on any newly developed system (or legacy system undergoing a major upgrade) before the system is authorized for operation; (ii) after important changes are made to the environment in which the system operates; and (iii) when a new type of attack is discovered that may impact the system. Organizations actively monitor the systems environment and the threat landscape (e.g., new vulnerabilities, attack techniques, new technology deployments, user security awareness and training) to identify changes that require penetration testing at various stages in the system life cycle.

VE-2-5: Conduct misuse testing to identify methods by which the system can be used as specified to produce unspecified emergent behavior that does not conform to security requirements.

Supplemental Guidance: Misuse testing verifies that guidance documents and procedures oriented to users, operators, administrators, and maintainers, when followed, produce the intended outcomes. Misuse testing is able to identify overly complex, erroneous, or ambiguous information that leads the user/operator/maintainer to inadvertently place the system in a non-secure state.

VE-2-6: Provide and protect system verification data in accordance with agreements and legal or regulatory requirements.

Supplemental Guidance: All system verification data is protected in the manner specified in agreements and by relevant legal and regulatory requirements.

VE-2-7: Analyze, record, and report security verification, discrepancy, and corrective action information.

Supplemental Guidance: Security verification data is collected, characterized, and collated according to the criteria defined in the security verification strategy. This data addresses non conformances by source, discrepancies, and any required corrective actions. Security verification data is analyzed to detect: (i) trends and patterns of vulnerabilities and security-relevant failures; (ii) security design errors; (iii) implementation weaknesses; and (iv) emerging threats to capability, data, and information processed, stored, or transmitted by the system. Security verification information is reported to stakeholders to: (i) obtain concurrence that the security-relevant elements have been built correctly and meet stakeholder security requirements; (ii) provide assurance that the security functions employed in the system will work as intended; and (iii) provide needed information to support risk-based decisions regarding the authorization to operate the system.

References: NIST Special Publication 800-53A.

## 3.7 TRANSITION PROCESS

***Purpose***

"The purpose of the *Transition Process* is to establish a capability to provide services specified by stakeholder requirements in the operational environment. This process installs a verified system, together with relevant enabling systems, e.g., operating system, support system, operator training system, user training system, as defined in agreements. This process is used at each level in the system structure and in each stage to complete the criteria established for exiting the stage. It includes preparing applicable storage, handling, and shipping enabling systems."



*Systems Security Engineering Purpose*

Systems security engineering, as part of the *Transition Process*, provides the capability to ensure that the specified protections for the system are in place as verified for use, and that appropriate protections are in place for the storage, handling, delivery installation, generation, configuration, and start-up of the verified system.

Systems Security Engineering Outcomes

The following *outcomes* can be expected from the successful execution of a security-enhanced Transition Process:

- The security strategy for transition is defined;
- A system is securely delivered, installed, and configured at its operational location;
- A system and its enabling systems are capable of delivering and sustaining the specified security services;
- The security configuration as installed, is recorded; and
- Corrective security action reports are recorded.

Systems Security Engineering Activities and Tasks

The following security-related *activities* are conducted as part of the Transition Process:

- Plan for the secure transition of the system; and
- Perform the secure transition of the system.

TR-1: PLAN FOR THE SECURE TRANSITION OF THE SYSTEM

TR-1-1: Prepare the strategy for secure transition of the system.

Supplemental Guidance: The secure transition strategy includes ensuring protections reflected in agreements are in place and effective to preserve the confidentiality and integrity of the system for all aspects of its transport, delivery, installation, generation, configuration and initial start-up. The secure transition strategy also accounts for interim storage protection needs, accountability of system elements throughout the transition process, and the security qualifications and authorizations of individuals associated with the transition of the system. The strategy for secure transition details the security measures necessary to provide assurance and establish trust that the security of the system is maintained throughout the transition process and activities to include: (i) ensuring that the delivered system corresponds precisely to the system verified; (ii) preventing and detecting actual and attempted tampering with the

system; (iii) preventing and detecting substitution or replacement of system elements; and (iv) preventing and detecting attempts to masquerade as authorized personnel associated with the transition process.

TR-1-2: Prepare the site of operation in accordance with installation security requirements, directives, policies, procedures, regulations, and local/site ordinances.

Supplemental Guidance: Site preparation for secure operation includes physical, personnel, procedural, and technical security measures implemented in accordance with stakeholder security requirements and agreements. Site preparation also includes the appropriate security training for operational personnel and the timely deployment of security-relevant administrator, maintenance, and user guidance, and security training to ensure the secure operation of the system.

References: ISO/IEC 15408; NIST Special Publications 800-53, 800-161.

### TR-2: PERFORM THE SECURE TRANSITION OF THE SYSTEM

TR-2-1: Deliver the system for installation at the specified location and time in accordance with the security measures described in the transition strategy.

Supplemental Guidance: Secure delivery of the system ensures that the integrity and confidentiality properties and other security attributes of the system and its constituent elements are preserved the entire time that the system is transferred from the development facility to the operational location. The delivery strategy is performed with tailoring to address threats and vulnerabilities specific to the decisions made and methods employed to deliver the system. The delivery procedures and mechanisms contain sufficient protections and assurances such that it is possible to: (i) ensure that the delivered system corresponds precisely to the system verified; (ii) prevent or detect actual/attempted tampering with the system; (iii) prevent or detect substitution or replacement of system elements; and (iv) prevent/detect attempts to masquerade as authorized personnel associated with the transition process.

TR-2-2: Install the system at its specified location and establish the interconnections that constitute trust relationships to its environment of operation in accordance with the system security specification and the security measures described in the transition strategy.

Supplemental Guidance: Installation, generation, and start-up procedures are useful for ensuring that the system has been installed, generated, configured, and securely integrated into its operational environment. Trust relationships between the system and other systems in its environment adhere to agreements, policies, and directives that govern approvals to connect and to interact with other systems, and with the stakeholder security requirements.

TR-2-3: Demonstrate proper installation, generation, configuration, and start-up of the system in accordance with the system security specification and security acceptance testing.

Supplemental Guidance: Trusted interconnections are verified before allowing any use of operational data and before allowing any interactions between the system and its environment. The demonstration of secure installation, generation, configuration, and start-up may be accomplished using verification and validation activities and criteria.

TR-2-4: Demonstrate that the installed system and its enabling systems are capable of delivering the required security services using the results of security acceptance tests, vulnerability assessments, penetration testing, and as specified in agreements.

Supplemental Guidance: The security transition strategy and the information generated during security acceptance testing, vulnerability assessments, and penetration testing provide evidence that the system and its enabling systems satisfy stakeholder security and security design requirements in the operational environment.

TR-2-5: Analyze, record, and report the security transition information, including results of security transition actions, nonconformance, and corrective actions taken.

Supplemental Guidance: The engineering team identifies any nonconformances associated with the system and its enabling systems and determines the impact of the nonconformance to the delivery of specified system security services. Options for corrective action are identified and a recommended course of action to remove the nonconformance is determined. The result of the corrective action is recorded and reported to stakeholders.

References: ISO/IEC 15408; NIST Special Publications 800-53, 800-161.

## 3.8 VALIDATION PROCESS

***Purpose***

"The purpose of the *Validation Process* is to provide objective evidence that the services provided by a system when in use comply with stakeholders' requirements, achieving its intended use in its intended operational environment. This process performs a comparative assessment and confirms that the stakeholders' requirements are correctly defined. Where variances are identified, these are recorded and guide corrective actions. System validation is ratified by stakeholders."



*Systems Security Engineering Purpose*

Systems security engineering, as part of the *Validation Process*, demonstrates that the *right* system was built. In particular, security validation demonstrates that the system protections: (i) are necessary, sufficient, and effective in protecting assets for the intended use of the system in its intended operational environment in accordance with the stakeholder security requirements; and (ii) are effective and able to enforce those portions of organizational security policy allocated to the system. Systems security engineering performs a protection-focused comparative assessment and confirms that: (i) the stakeholder security requirements are correctly defined; (ii) the security requirements are correctly realized in the system design and implementation; (iii) the system is able to enforce organizational security policy while providing continuous protection in all defined system modes of operation; (iv) system protections are sufficiently resistant to attack and misuse; and (v) trustworthiness objectives of stakeholders have been achieved. Additionally, security validation identifies vulnerabilities and determines how those vulnerabilities may be exploited or triggered by threat events, thereby determining the susceptibility to threat that can be expected during operations and sustainment.

Systems Security Engineering Outcomes

The following *outcomes* can be expected from the successful execution of a security-enhanced Validation Process:

- A security strategy for validation is defined;
- The availability of security services required by stakeholders is confirmed;
- Security validation data is provided; and
- Data sufficient to inform security-relevant corrective actions is documented and reported.

Systems Security Engineering Activities and Tasks

The following security-related *activities* are conducted as part of the Validation Process:

- Plan the security validation of the system; and
- Perform security validation of the system.

VA-1: PLAN THE SECURITY VALIDATION OF THE SYSTEM

VA-1-1: Define the strategy for validating the end-to-end security protections and security services in the operational environment and for achieving stakeholder security satisfaction.

Supplemental Guidance: The validation process ensures that the right system was built and that it is fit for the purpose and intended use by stakeholders to protect mission/business assets. Security validation demonstrates that the system: (i) satisfies stakeholder security requirements; (ii) is able to continuously enforce security policy in all defined system modes of operation; (iii) possesses no unspecified behavior to the degree possible; (iv) is sufficiently resistant to attack and misuse; and (v) satisfies the trustworthiness objectives of stakeholders. Security validation can also demonstrate: (i) correctness of security functionality; (ii) specified strength of function/mechanism; (iii) compliance with concepts of operation, performance, and interoperability; and (iv) residual vulnerabilities and how those vulnerabilities may be exploited or triggered by threat events, thereby determining the susceptibility to threat that can be expected during operations and sustainment. Security validation is conducted in all system life cycle stages as an activity tied to each of the technical engineering processes for developmental and field engineering efforts to demonstrate that the engineering efforts and outcomes are contributing to the satisfaction of stakeholder protection needs, expectations, trustworthiness, and risk concerns. Security validation activities include determining what constitutes relevant and credible evidence sufficient to support conclusions that assurance, trustworthiness, and risk claims are achieved. Security validation may also specify activities to generate or obtain the evidence, and the analyses conducted to qualify, assess, and reach conclusions based on the evidence. Security validation may employ various techniques and methods (e.g., observation, inspection, test) to generate evidence that reflects conclusive objective results (e.g., pass/fail), and provides evidence used in analyses that can substantiate arguments for subjective results and claims.

VA-1-2: Define a security validation plan based on stakeholder security requirements.

Supplemental Guidance: The security validation plan defines security validation steps that are applied to accomplish specific mission/business objectives during specified operational states and scenarios. Security validation evidence that is produced during the security validation process progressively builds assurance (i.e., confidence) to provide a basis for determining the trustworthiness and risk associated with the installed system and to assist in determining security-relevant weaknesses or discrepancies. Methods and techniques needed to implement the security validation strategy are specified, as are the purpose, conditions, and conformance criteria for each security validation carried out during the various stages of the system life cycle. Where stakeholder security requirements cannot be specified comprehensively or change frequently, repeated security validation of increments in system evolution may be used to refine stakeholder security requirements and mitigate security risks in the correct identification of protection needs.

References: None.

### VA-2: PERFORM SECURITY VALIDATION OF THE SYSTEM

VA-2-1: Ensure that the enabling systems, test suites, equipment, simulators, facilities, and personnel used for security validation are available and prepared to conduct the validation.

Supplemental Guidance: Security validation activities may require specialized tools and the application of certain techniques that require specialized expertise and skills.

VA-2-2: Conduct security validation to demonstrate that the system protections conform to stakeholder security requirements and are effective given the mission/business concept of operation and the intended use of the system.

Supplemental Guidance: Security validation confirms that the right system was built as determined by the stakeholders. That is, security validation is conducted with sufficient breadth and depth (i.e., specificity) to account for demonstration that stakeholder security requirements have been satisfied and that stakeholder mission/business protection needs and expectations have been met. Security validation is conducted at various levels (e.g., mechanism, function, component, service, subsystem, system, and system-of-systems) and includes technical, physical, and procedural elements of the system, as well as all supporting life cycle processes for development, supply chain, operations, and sustainment of the system. Security validation is conducted on individual system elements and on combinations of elements based on the partitioning and trust relationships expressed in the security architectural design of the system, and in terms of system elements and how those elements interact within the system. In addition, security validation continuously builds the base of evidence required to substantiate claims of satisfying stakeholder protection needs and security requirements and the enforcement of security policy within the broader capability and performance constraints of the system. Security validation is conducted in accordance with a specific validation strategy put in place during requirements elicitation and analysis, and is updated as the system design matures and during the system life cycle. Corrective actions are initiated as appropriate to resolve demonstrated noncompliance. Security validation is undertaken in a manner consistent with organizational constraints, such that uncertainty in the replication of security validation actions, conditions, and outcomes is minimized. Security validation actions and outcomes are documented and approved.

VA-2-3: Conduct a vulnerability assessment to identify exploitable vulnerabilities and vulnerabilities that may be triggered by errors of omission, commission, or by system faults and failures.

Supplemental Guidance: Vulnerability assessments are conducted at various stages in the system life cycle in support of systems engineering and systems security engineering efforts. See *Verification Process* Task VE-2-3 for additional information on the conduct of vulnerability assessments.

VA-2-4: Conduct penetration testing to identify exploitable vulnerabilities and to determine the residual susceptibility to specific malicious threat events.

Supplemental Guidance: Penetration testing is conducted at various stages in the system life cycle in support of systems engineering and systems security engineering efforts. See the *Verification Process* for additional information on the conduct of penetration testing.

VA-2-5: Conduct misuse testing to identify methods by which the system can be used as specified but results in a violation of security policy or unspecified system behavior.

Supplemental Guidance: Misuse testing is conducted at various stages in the system life cycle in support of systems engineering and systems security engineering efforts. See the *Verification Process* for additional information on the conduct of misuse testing.

VA-2-6: Make available security validation data on the system and obtain stakeholder concurrence.

Supplemental Guidance: Security validation data collected by the engineering team or the independent entity conducting the validation can be made available to stakeholders: (i) to explain how the system meets the stakeholder security requirements and protection needs, the results of the implementation and integration verification activities, and the residual risks associated with the system; and (ii) to obtain approval and concurrence to proceed with submitting the system for authorization for use in the operational environment. The evidence generated during the validation process demonstrates to the key stakeholders the effectiveness and completeness of the system in addressing the stakeholder security requirements and protection needs. This includes ensuring that key stakeholders understand the decisions that contributed to the system design and implementation and the associated risks. This enables stakeholders to determine operational risks and mission/business impact, and their options and responsibility for mitigating and monitoring risk during the operational use of the system.

VA-2-7: Analyze, record, and report security validation information in accordance with the criteria defined in the security validation plan.

Supplemental Guidance: Security verification data is collected, characterized, and collated according to the criteria defined in the security verification strategy. This data addresses nonconformances by source, discrepancies, and any required corrective actions. Security verification data is analyzed to detect: (i) trends and patterns of vulnerabilities and security-relevant failures; (ii) security design errors; (iii) implementation weaknesses; and (iv) emerging threats to capability, data, and information processed, stored, or transmitted by the system.

References: NIST Special Publication 800-53A.

## 3.9 OPERATION PROCESS

***Purpose***

"The purpose of the *Operation Process* is to use the system in order to deliver its services. This process assigns personnel to operate the system, and monitors the services and operator-system performance. In order to sustain services, it identifies and analyzes operational problems in relation to agreements, stakeholder requirements and organizational constraints."



*Systems Security Engineering Purpose*

Systems security engineering, as part of the *Operation Process*, plans for the engineering that takes place to enable the secure operation of the system and provides field engineering support to operational organizations to address security incidents, failures, and related considerations that require systems engineering involvement. Systems security engineering: (i) determines the secure operations constraints on requirements and architectural design; (ii) identifies the capabilities, skills, and experience necessary for security personnel that are responsible to operate and to interact with the protection-related portions of the system; (iii) identifies and analyzes problems that occur during operations to determine the security relevance; (iv) performs field engineering services in direct support of operations to design and employ field modifications/enhancements; and (v) identifies and analyzes security-relevant data and information that is monitored and collected during operations.

Systems Security Engineering Outcomes

The following *outcomes* can be expected from the successful execution of a security-enhanced Operation Process:

- A strategy for secure operations is defined;
- Security-relevant operations constraints are provided as input to requirements and architectural design;
- Services that meet stakeholder security requirements are delivered;
- Security-relevant corrective actions are satisfactorily completed; and
- Stakeholder protection needs satisfaction is maintained.

Systems Security Engineering Activities and Tasks

The following security-related *activities* are conducted as part of the Operation Process:

- Prepare for the secure operation of the system;
- Perform security operational activation and check out the system;
- Use the system to secure operations;
- Perform operational security problem resolution; and
- Support the customer to provide continuous protection of assets.

OP-1: PREPARE FOR THE SECURE OPERATION OF THE SYSTEM

OP-1-1: Prepare a strategy for secure operation of the system.

Supplemental Guidance: The operational security strategy accounts for the continuous secure use of security services: (i) once the services are activated or enabled; (ii) while the services are in operation; and (iii) until the services are terminated. The operational secure system state is achieved from the proper and continuous enforcement of security policy at the system level. This is achieved by a strategy that: (i) establishes/maintains the secure system configuration; (ii) determines that the system security behavior is as intended; (iii) determines that personnel adhere to established security procedures; and (iv) accounts for the proper employment and use of physical protections. The development of the secure operational strategy requires coordination with preexisting, concurrent, and continuing systems, security services, security architectures, and infrastructures provided by other systems to ensure that security configurations, roles, and responsibilities are understood. The strategy encompasses: (i) the identification of the operational security-driven constraints on developmental and field engineering, on operations, and for modifications to enhance or sustain the system security services; (ii) the engineering of the security functional capability needed to support organizational continuous monitoring objectives; (iii) the development of policies and procedures needed to perform continuous monitoring of the security state of the system; and (iv) the determination of the requirements, architecture, and design changes necessary to remediate deficiencies identified once the system is operational. The strategy also addresses the data and information collected during operations to support: (i) the establishment and preservation of a secure system state; (ii) threat, vulnerability, and risk monitoring; (iii) detection of attacks and the activities of insider and external threat agents; (iv) response to realized attacks and to the impact of errors, fault, and failures; and (v) post-security-incident forensic analyses.

OP-1-2: Obtain other services related to the secure operation of the system.

Supplemental Guidance: The planning for operations considers other services/support services related to the secure operation of the system to include: (i) human resource services providing background checks on personnel with operational responsibilities regarding the secure operation and maintenance of the system; and (ii) contingency planning and continuity of operations services providing alternate processing capability, alternate communications capability, and alternate storage capability. All dependent and supporting services are identified during requirements elicitation, analysis, and architectural design with consideration of the strategy for secure operation.

OP-1-3: Establish criteria to train and qualify personnel to securely operate the system.

Supplemental Guidance: Secure systems operation requires appropriate training and qualification of personnel. Qualifications may include, for example, the determination of clearances, background checks, and other security-related criteria required for personnel with responsibility for security management and system operation. Security training is provided for all personnel that interact directly or indirectly with the system. Such training includes security awareness training to supplement the training of personnel to understand and to properly use the protections as they were designed to be used. The scope of security training includes protections implemented in the system and the operational environment, and the responsibility for personnel to understand and adhere to security procedures.

References: None.

OP-2: PERFORM SECURITY OPERATIONAL ACTIVATION OF THE SYSTEM

OP-2-1: Activate the system in its environment of operation to deliver secure services in accordance with the intended purpose of the system.

Supplemental Guidance: The system is activated in accordance with the secure installation, generation, and start-up procedures as described in the Transition Process. The system is activated only after successfully completing security validation of the operational configuration and when the system is delivering security services and protections as intended by the stakeholder security requirements.

OP-2-2: Verify that the system is operating as specified.

Supplemental Guidance: As part of system activation, the engineering team: (i) verifies that system interactions over internal and external interconnections reflect trust relationship criteria for the secure exchange of data/information, to include trust relationships relied upon for secure system management; and (ii) verifies that the system is effective in providing for its own self-protection, in protecting mission/business assets, and in its enforcement of organizational security policy. For the case of system changeover or concurrent system operation, continuous security service capacity and quality is maintained. The transfer of security services is managed so that continuing conformance to stakeholder protection needs is achieved.

References: None.

### OP-3: USE THE SYSTEM TO SECURE OPERATIONS

OP-3-1: Monitor system operations to ensure that the system: (i) is being used in accordance with its stated purpose; (ii) is being operated in a secure manner consistent with the security concept of operations; and (iii) is compliant with security- and privacy-relevant legislation, Executive Orders, directives, regulations, policies, and procedures.

Supplemental Guidance: Monitoring the system to ensure that it is being used only for its intended purpose helps to reduce the susceptibility to threats by limiting exposure of vulnerabilities to untrusted or unknown entities. The operational security strategy serves to guide secure use and monitoring of the system.

OP-3-2: Monitor system operations to confirm that service performance is within acceptable security parameters and to detect vulnerabilities.

Supplemental Guidance: Given that the system is being used correctly, additional monitoring is necessary to ensure that the system is delivering the required protection despite attacks, faults, failures, environmental events, incidents, and accidents. Such monitoring helps to detect potential attacks, intrusions, and insider threat activity, and to confirm that the system continues to operate in a secure configuration and in a secure state. Security monitoring also applies to the capabilities of individuals operating the system to ensure that they continue to possess the requisite security-related skills and expertise to effectively operate and/or use the system in a secure manner. The operational security strategy serves to guide secure use and monitoring of the system.

OP-3-3: Monitor system operations to detect adversarial activity.

Supplemental Guidance: Given that the system is being used correctly and that security protections and services are performing within acceptable parameters, additional monitoring is necessary to actively identify the actions, behavior, and attempts of threat agents (attackers). The operational security strategy serves to guide secure use and monitoring of the system.

References: None.

### OP-4: PERFORM OPERATIONAL SECURITY PROBLEM RESOLUTION

OP-4-1: Identify security failures that affect the delivery of system services or the conduct of secure system operations.

Supplemental Guidance: Security protection and service failures include: (i) technology-based (e.g., hardware, software, firmware); (ii) procedural-based (e.g., policies, procedures); or (iii) personnel-based (e.g., operators, administrators). The context of security failures are the stakeholder security requirements, security design requirements, and organizational security policy. The inability to satisfy a requirement or to properly enforce organizational security policy constitutes a security failure condition. Attacks, incidents, or accidents are the ways to express security failures.

OP-4-2: Determine the appropriate course of action to respond to a security failure and implement remediation.

Supplemental Guidance: A security course of response action is conducted: (i) when a security failure occurs; or (ii) when there is a failure in system services or the routine execution of the system that may be caused by a security failure. Courses of action may involve: (i) changes to stakeholder protection needs and/or security requirements; (ii) changes to security architectural design and/or implementation; (iii) changes to hardware, software, or firmware; (iv) changes to policies or procedures; (v) changes to the security concept of operations; or (vi) accepting diminished services until a cost-effective and risk-acceptable course of action can be determined and implemented. For security failures that involve individuals (i.e., human errors of omission or commission), changes may also be needed in personnel security training, user interfaces, and/or the security-relevant features of the operating environment.

References: None.

OP-5: SUPPORT THE CUSTOMER TO PROVIDE CONTINUOUS PROTECTION OF ASSETS

OP-5-1: Establish a mechanism for continuous communication with stakeholders and improvement in the security-relevant aspects of the system.

Supplemental Guidance: Continuous communication with stakeholders provides the feedback loop that is necessary for continuous improvement in system security protection and security services. The need for improvement is influenced by: (i) stakeholder issues regarding the effectiveness and sufficiency of security protections and services; (ii) security protections and services which hinder achievement of mission/business objectives; (iii) changes to system hardware, software, or firmware components; (iv) changes to the system environment of operation; or (v) nonconformance to governing legislation, Executive Orders, directives, regulations, or policies. The response to an identified need for improvement in the system is accomplished by executing all necessary systems security engineering processes as part of developmental and field engineering.

References: None.

## 3.10 MAINTENANCE PROCESS

***Purpose***

"The purpose of the *Maintenance Process* is to sustain the capability of the system to provide a service. This process monitors the system's capability to deliver services, records problems for analysis, takes corrective, adaptive, perfective and preventive actions and confirms restored capability."



*Systems Security Engineering Purpose*

Systems security engineering, as part of the *Maintenance Process*, plans for the engineering that takes place to enable secure maintenance of the system and provides field engineering support to maintenance organizations to sustain system protections and security services. Systems security engineering: (i) determines the secure maintenance constraints on requirements and architectural design; (ii) identifies the skills, capabilities, and experience necessary for maintenance personnel that are responsible to service and maintain the system; (iii) identifies and analyzes reported problems and incidents to determine security relevance; (iv) performs field engineering services in direct support of maintenance to design and employ field modifications and enhancements; (v) identifies and analyzes security-relevant evidence (e.g., data, information, problem and incident reports) to be monitored, collected, and analyzed to support secure system maintenance; and (vi) confirms restored security capability.

Systems Security Engineering Outcomes

The following *outcomes* can be expected from the successful execution of a security-enhanced Maintenance Process:

- A strategy for the secure maintenance of the system is defined;
- Security-relevant maintenance constraints are provided as input to requirements and architectural design;
- Security-relevant replacement system elements are made available;
- Services meeting stakeholder security requirements are sustained;
- The need for corrective security design changes is reported;
- Security qualifications for maintenance personnel are defined;
- Security criteria for maintenance tools are identified; and
- Security failure data is recorded, reported, and maintained for the life of the system.

Systems Security Engineering Activities and Tasks

The following security-related *activities* are conducted as part of the Maintenance Process:

- Plan for the secure maintenance of the system; and
- Perform secure maintenance on the system.

MA-1: PLAN FOR THE SECURE MAINTENANCE OF THE SYSTEM

MA-1-1: Prepare a strategy for the secure maintenance of the system.

Supplemental Guidance: The secure maintenance strategy: (i) identifies the operational security-driven constraints on developmental and field engineering, on operations, and for modifications to enhance or sustain the system security services; (ii) defines the performance of system maintenance using qualified personal and qualified maintenance tools in conformance with security design requirements and the organizational security policy; and (iii) describes the performance of maintenance activities in accordance with manufacturer/vendor specifications and/or organizational requirements to include security considerations for the control and monitoring of remote maintenance activities. The maintenance strategy helps to ensure that: (i) maintenance activities can be performed to achieve intended outcomes regardless of the location at which maintenance is performed; (ii) the confidentiality and integrity of data/information is preserved throughout all aspects of maintenance; and (iii) all system protections and security services are verifiably intact following system maintenance activities.

MA-1-2: Determine the security criteria for system maintenance tools.

Supplemental Guidance: The engineering team determines the security criteria for the selection and/or approval of maintenance tools for use on the system. Maintenance tools are those tools used specifically for diagnostic, analysis, and simulation to support the repair of system elements and any other tool or device connected to the system during the course of maintenance activities. Maintenance tools are potential vehicles for altering system hardware, software, and firmware components to enable or facilitate an attack on the system.

MA-1-3: Determine the security qualification for maintenance personnel.

Supplemental Guidance: The engineering team identifies the security qualifications and competencies of individuals who perform maintenance on the systems and for individuals requiring physical access to the system to perform required maintenance duties.

References: None.

MA-2: PERFORM SECURE MAINTENANCE ON THE SYSTEM

MA-2-1: Conduct system maintenance in accordance with the secure maintenance strategy.

Supplemental Guidance: The engineering team works with maintenance and operational personnel to accomplish system maintenance in a manner that does not conflict with the protection of system assets, and to the level of detail included in system maintenance records informed by the mission/business function being supported by the system. The integrity of maintenance tools and supporting tools that are connected to the system during maintenance are verified to ensure that the tools have not undergone erroneous, improper, or unauthorized modification which could adversely affect the ability of the system to provide its specified protections/security services. Secure maintenance encompasses the entire system and is not limited to security-relevant system elements. In particular, routine and periodic preventive maintenance activities are performed as directed by a maintenance schedule. These preventive maintenance actions may involve removal, disassembly, inspection, and reassembly of system components. Partial or complete component replacement may be required based on what is discovered during the maintenance inspection. The opportunity for incidental, accidental, or intentional tampering with system components is possible during preventive maintenance.

MA-2-2: Initiate corrective security action to remedy previously undetected security design errors and oversights.

Supplemental Guidance: The engineering team conducts analysis of evidence collected and identifies security design errors and oversights that require security developmental engineering actions to resolve. Recommendations to correct the identified errors and oversights are provided as options to the developmental engineering teams.

MA-2-3: Document security-relevant maintenance activities, the need for corrective action, and the corrective action that was performed.

Supplemental Guidance: The engineering team documents information for the maintenance team regarding the types of events, actions, or activities during the maintenance process that could adversely affect the security properties of the system. Such events, actions, or activities are conveyed by the field engineering team to the developmental engineering team in the situation where developmental corrective actions are required.

References: None.

## 3.11 DISPOSAL PROCESS

***Purpose***

"The purpose of the *Disposal Process* is to end the existence of a system entity. This process deactivates, disassembles, and removes the system and any waste products, consigning them to a final condition and returning the environment to its original or an acceptable condition. This process destroys, stores, or reclaims system entities and waste products in an environmentally sound manner, in accordance with legislation, agreements, organizational constraints, and stakeholder requirements. Where required, it maintains records in order that the health of operators and users, and the safety of the environment, can be monitored."



*Systems Security Engineering Purpose*

Systems security engineering, as part of the *Disposal Process*, plans for and provides engineering support to accomplish the secure deactivation, disassembly, removal, and reuse of the system. Systems security engineering identifies the appropriate protections and/or sanitization methods employed for handling of sensitive components, data, and information, and that destruction of system elements is accomplished to securely destroy sensitive technology, data, and information.

Systems Security Engineering Outcomes

The following *outcomes* can be expected from the successful execution of a security-enhanced Disposal Process:

- A secure system disposal strategy is defined;
- Security-relevant disposal constraints are provided as input to requirements and architectural design;
- Mission/business assets, system elements, and waste products are securely destroyed, reclaimed, stored, or recycled; and
- Secure disposal actions and analysis results of long-term vulnerability and susceptibility to threats are documented and archived.

Systems Security Engineering Activities and Tasks

The following security-related *activities* are conducted as part of the Disposal Process:

- Plan for the secure disposal of the system; and
- Perform secure disposal of the system.

DS-1: PLAN FOR THE SECURE DISPOSAL OF THE SYSTEM

DS-1-1: Prepare a strategy for the secure disposal of the system, to include each system element, system and stakeholder material, data, and information assets.

Supplemental Guidance: The secure disposal strategy ensures that sensitive components, technology, information, and data have appropriate confidentiality, integrity, and availability protections when removed from service, dismantled, stored, prepared for reuse, and destroyed. The protection needs during disposal are equivalent to or derived from those protections put in place as a result of the protection needs assessment. The security aspects of the disposal strategy

account for: (i) the permanent termination of the system's delivery of services; (ii) transforming the system into, or retain it in, an acceptable storage state; and (iii) sensitivity and privacy concerns determined by the nature of the mission/business supported by the system.

DS-1-2: Define the constraints on system requirements and system design that are unavoidable consequences of the secure disposal strategy.

Supplemental Guidance: Procedures for secure disposal may be constrained by aspects of the system design and may dictate constraints on system requirements and design. Conformance with regulatory requirements for secure disposal may also dictate constraints on system requirements and system design, to include, for example, the procedures that are to be followed by personnel conducting system disposal activities.

DS-1-3: Specify secure storage criteria for the elements of the system, mission/business assets, and system assets to be stored.

Supplemental Guidance: The criteria includes authorized facilities and locations for secure storage, the authorized length of storage, storage verification checks, audits, and inspections, and the period after which the secure storage criteria is no longer applicable.

References: None.

DS-2: PERFORM SECURE DISPOSAL OF THE SYSTEM

DS-2-1: Acquire the enabling systems or services to be used during secure disposal of a system.

Supplemental Guidance: None.

DS-2-2: Deactivate the system to prepare it for secure removal from operation.

Supplemental Guidance: System deactivation is to be accomplished so as to not expose connected systems to threats when trusted interconnections are severed. All system deactivation procedures and activities are to be accomplished such that the protection of assets is maintained until such time that alternative protections are put in place as determined by the secure disposal strategy and agreements.

DS-2-3: Conduct security debriefings, revoke authorizations for access to sensitive system material and information assets, and collect all sensitive data, information, and material assets from system user, operations, maintenance, and support personnel.

Supplemental Guidance: None.

DS-2-4: Sanitize security-relevant system elements prior to disposal, release out of organizational control, or release for reuse.

Supplemental Guidance: Sanitization techniques include clearing, purging, cryptographic erase, and physical destruction, and serve to prevent the disclosure of information to unauthorized individuals should media be reused or released for disposal. Sanitization applies to all system elements, assets, and technology. The sanitization process has the means to determine that information content cannot be retrieved or reconstructed.

DS-2-5: Ensure appropriate protections are in place for system components, data, and information during removal, reuse, recycling, reconditioning, overhaul, or destruction.

Supplemental Guidance: None.

DS-2-6: Verify that all identified sensitive material and information assets have been accounted for and have been properly disposed of, stored, or placed in a new environment of operation.

Supplemental Guidance: Secure destruction of data, information, and material assets is in accordance with agreements and relevant security and privacy legislation, directives, or policies and pose no unacceptable security risk associated with unauthorized exfiltration, access, or loss of sensitive assets.

DS-2-7: Verify that all archived information has sufficient security and privacy protections in place, to include periodic reviews and audits to determine when protections are no longer required or when the archived information may be securely destroyed.

Supplemental Guidance: None.

References: None.

APPENDIX A

# REFERENCES

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

**LEGISLATION AND EXECUTIVE ORDERS**

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
3. USA PATRIOT Act (P.L. 107-56), October 2001.

**POLICIES, DIRECTIVES, INSTRUCTIONS, REGULATIONS, AND MEMORANDA**

1. Committee on National Security Systems Policy (CNSSP) No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products*, July 2003.
2. Committee on National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, April 2010.
3. Office of Management and Budget Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.
4. Office of Management and Budget, *The Common Approach to Federal Enterprise Architecture*, May 2012.
5. Office of Management and Budget, *Federal Enterprise Architecture*, Version 2.0, January 2013.
6. Office of Management and Budget, *Federal Segment Architecture Methodology (FSAM)*, January 2009.

**STANDARDS**

1. International Organization for Standardization/International Electrotechnical Commission 15408-1:2009, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model*.
2. International Organization for Standardization/International Electrotechnical Commission 15408-2:2008, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements*.
3. International Organization for Standardization/International Electrotechnical Commission 15408-3:2008, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements*.
4. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
5. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

6. Institute of Electrical and Electronic Engineers (IEEE), IEEE Standard Glossary of Software Engineering Terminology, IEEE Std 610.12-1990, Institute of Electrical and Electronic Engineers, 1990.
7. Institute of Electrical and Electronic Engineers (IEEE), IEEE Std 15026-1-2010, Systems and Software Engineering—Systems and Software Assurance—Part 1: Systems and Software Engineering—Systems and Software Assurance—Part 1: Concepts and Vocabulary, Institute of Electrical and Electronic Engineers, 2011. (Adoption of ISO/IEC TR 15026-1 Part 1:2010.)
8. International Organization for Standardization (ISO) Guide 73:2009, 31000, *Risk Management—Vocabulary*, *International Organization for Standardization*, 2009.
9. International Organization for Standardization/International Electrotechnical Commission, ISO/IEC 15288, IEEE Std 15288-2008 *Systems and Software Engineering—Systems Life Cycle Processes*, 2008.

**GUIDELINES AND INTERAGENCY REPORTS**

1. National Institute of Standards and Technology Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, September 2012.
2. National Institute of Standards and Technology Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010.
3. National Institute of Standards and Technology Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.
4. National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.
5. National Institute of Standards and Technology Special Publication 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, June 2010.
6. National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.
7. National Institute of Standards and Technology Special Publication 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.
8. National Institute of Standards and Technology Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011.

APPENDIX B

# GLOSSARY

COMMON TERMS AND DEFINITIONS

Appendix B provides definitions for engineering and security terminology used within Special Publication 800-160. Unless specifically defined in this glossary, terms used in this publication are consistent with the definitions contained in CNSS Instruction 4009, *National Information Assurance Glossary*.

| | |
|---|---|
| Advanced Persistent Threat | An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information; undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives [NIST SP 800-53]. |
| Analysis of Alternatives | An analytical comparison or evaluation of proposed approaches to meet an objective. An analysis of alternatives can be applied to anything—from a large military acquisition decision to a decision between two products. The formal or informal process involves identifying key decision factors, such as life cycle operations, support, training, and sustainment costs, risk, effectiveness, and assessing each alternative with respect to these factors.<br>An analysis of alternatives is an analytical comparison of the operational effectiveness, cost, and risks of proposed materiel solutions to gaps and shortfalls in operational capability. Such analyses document the rationale for identifying/recommending a preferred solution or solutions to the identified shortfall. Threat changes, deficiencies, obsolescence of existing systems, or advances in technology can trigger an analysis of alternatives. |
| Architecture | A set of related physical and logical representations (i.e., views) of a system or a solution. The architecture conveys information about system/solution elements, interconnections, relationships, and behavior at different levels of abstractions and with different scopes.<br>Refer to *Security Architecture.* |

| | |
|---|---|
| Architecture Trade-off Analysis | A method for evaluating architecture-level designs that considers multiple quality attributes such as modifiability, performance, reliability, and security in gaining insight as to whether the fully described architecture will meet its requirements. The method identifies trade-off points between these attributes, facilitates communication between stakeholders (such as user, developer, customer, maintainer) from the perspective of each attribute, clarifies and refines requirements, and provides a framework for an ongoing, concurrent process of system design and analysis. |
| Asset | An item of value to achievement of organizational mission/business objectives.<br>A major application, general support system, high-impact program, physical plant, mission-critical system, personnel, equipment, or a logically related group of systems [CNSSI-4009].<br>*Note 1:* Assets have interrelated characteristics that include value, criticality, and the degree to which they are relied upon to achieve organizational mission/business objectives. From these characteristics, appropriate protections are to be engineered into solutions employed by the organization.<br>*Note 2:* An asset may be tangible (e.g., physical item such as hardware, software, computing platform, network device, and other technology components) or intangible (e.g., information, data, trademark, copyright, patent, intellectual property, software, image, or reputation). |
| Assurance | Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy [CNSSI 4009, NIST SP 800-39].<br>Grounds for justified confidence that a claim has been or will be achieved [IEEE 15026-1:2010].<br>*Note 1:* Assurance is typically obtained relative to a set of specific claims. The scope and focus of such claims may vary (e.g., security claims, safety claims) and the claims themselves may be interrelated.<br>*Note 2:* Assurance is obtained through techniques and methods that generate credible evidence to substantiate claims.<br>Refer to *Assurance Evidence, Claims, Evidence.* |
| Assurance Evidence | The credible evidence upon which decisions regarding assurance, trustworthiness, and risk of the solution are substantiated.<br>*Note:* Assurance evidence is specific to an agreed-to set of claims. The security perspective focuses on assurance evidence for security-relevant claims whereas other engineering disciplines may have their own focus (e.g., safety).<br>Refer to *Evidence*. |

| | |
|---|---|
| Authorization (to operate) | The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. |
| Authorization Boundary | All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected [CNSSI-4009; NIST SP 800-37].<br>*Note:* The authorization boundary typically determines the boundary of the system-of-interest.<br>Refer to *System-of-Interest.* |
| Authorizing Official | The key stakeholder with the responsibility and authority to determine that the system delivered by the engineering effort meets its requirements and may be offered for use.<br>A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation [NIST SP 800-37]. |
| Availability | Ensuring timely and reliable access to and use of information [44 U.S.C., Sec. 3542; NIST SP 800-53; FIPS 199].<br>The property of being accessible and useable upon demand by an authorized entity [CNSSI 4009].<br>*Note:* Mission/business assurance resiliency objectives extend the concept of availability to refer to a point-in-time availability (i.e., the device is usable when needed) and the continuity of availability (i.e., the device remains usable for the duration of the time it is needed). |
| Baseline | A specification or work product that has been formally reviewed and agreed-upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures [ISO/IEC/IEEE 15288].<br>*Note:* The engineering process generates many artifacts that are maintained as a baseline over the course of the engineering effort and after its completion. The configuration control processes of the engineering effort manage baselined artifacts. Examples include stakeholder requirements baseline, system requirements baseline, architecture/design baseline, and configuration baseline.<br>Refer to *Stakeholder Requirements Baseline.* |
| Body of Evidence | The totality of evidence used to substantiate trust, trustworthiness, and risk relative to the system.<br>Refer to *Assurance Evidence, Evidence.* |

| | |
|---|---|
| Claims | Statement of something to be true, including associated conditions and limitations [ISO/IEC 15026]. |
| Confidentiality | Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information [44 U.S.C., Sec. 3542]. |
| Constraints | Factors that impose restrictions and limitations on the system.<br>Actual limitations associated with the use of the system.<br>Constraints may result as the consequences of existing agreements, management decisions, technical decisions, technology limitations, or the operational environment [adapted from Sections 6.4.1 and 6.4.2 of ISO/IEC/IEEE 15288:2008].<br>*Note:* Constraints are generally associated with characteristics of the environment specific to the various domains associated with the system. |
| Criticality | An attribute assigned to an asset that reflects its relative importance or necessity in achieving or contributing to the achievement of mission/business goals. |
| Defense-in-Breadth | A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement) [CNSSI 4009]. |
| Defense-in-Depth | Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization [CNSSI 4009]. |
| Derived Requirement | A requirement that is implied or transformed from higher-level requirement(s) [DAU Systems Engineering Fundamentals].<br>*Note 1:* Implied requirements cannot be assessed since they are not contained in any requirements baseline. The decomposition of requirements throughout the engineering process makes implicit requirements explicit, allowing them to be stated and captured in appropriate baselines and allowing associated assessment criteria to be stated.<br>*Note 2:* A derived requirement must trace back to at least one higher-level requirement. |

| | |
|---|---|
| Design Trade-off Analysis | Analysis that is focused on determining the design approach that is best suited for implementing the elements, physical safeguards, and procedural measures of the system.<br>*Note:* A design trade-off analysis includes the following considerations: (i) whether technical elements, physical safeguards, or procedural measures are appropriate to implement the system security requirements; and (ii) whether acquiring an off-the-shelf product, accessing or developing a service, or custom development is appropriate to implement the system security requirements. |
| Environment of Operation | The physical surroundings in which an information system processes, stores, and transmits information [NIST SP 800-37].<br>*Note:* The environment of operation is also referred to as the operational environment. |
| Evidence | Grounds for belief or disbelief; data on which to base proof or to establish truth or falsehood.<br>*Note 1:* Evidence can be objective or subjective. Evidence is obtained through measurement, the results of analyses, experience, and the observation of behavior over time<br>*Note 2:* The security perspective places focus on credible evidence used to obtain assurance, substantiate trustworthiness, and assess risk.<br>Refer to *Assurance Evidence, Body of Evidence*. |
| External Information System (or component) | An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness [CNSSI 4009].<br>*Note:* The term external should not be interpreted as or equated to meaning physically external. A distributed system will have elements that are physically/geographically distributed while being logically within the same authorization boundary. |
| Independent Verification and Validation (IV&V) | Verification and validation (V&V) performed by an organization that is technically, managerially, and financially independent of the development organization [IEEE Std 610.12-1990].<br>Refer to *Verification and Validation (V&V).* |
| Information | Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual [CNSS 4009].<br>*Note:* Data includes sensor data, configuration, command, and control data, financial data, personal data, images, audit logs, weapons data, encrypted data, etc. |

| | |
|---|---|
| Information Assurance | The measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities [CNSSI-4009]. |
| Information Management Model | A model that reflects the mission/business processes and how information is accessed, processed, transmitted, and stored to support those processes. The information management model provides the foundation for security-focused analyses that aid in determination of the stakeholder security requirements. |
| Information Protection Policy | An artifact of the systems security engineering process that captures the results of security-relevant analyses, the stakeholder security requirements, and other security-relevant information.<br>*Note:* The stakeholder security requirements can be regarded as a form of policy in the sense that those requirements combine to express the rules explicitly without ambiguity regarding what is allowed and what is not allowed. |
| Information System | A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information [CNSSI 4009].<br>Refer to *System.* |
| Infrastructure | A collection of interconnected elements that provide common facilities and services, or that enable the provision of common facilities and services. |
| Integrity | Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity [44 U.S.C., Sec. 3542].<br>The property whereby an entity has not been modified in an unauthorized manner [CNSSI-4009].<br>Data Integrity: The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner [CNSSI 4009].<br>System Integrity: Attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system [CNSSI 4009]. |
| Least Privilege Analysis | Activity that determines the minimum set of privileges required by individuals, processes, and services to achieve their purpose in support of the mission/business. The analysis determines the attributes to be used in the enforcement of security policy governing access to and the use of the mission/business functions, information, systems, and services. |
| Life Cycle | Evolution of a system, product, service, project, or other human-made entity from conception through retirement [ISO/IEC/IEEE 15288–2008]. |

| | |
|---|---|
| Life Cycle Stages | The major life cycle periods associated with a system. Each stage has a distinct purpose and contribution to the whole life cycle and is considered when planning and executing the system life cycle. The stages describe the major progress and achievement milestones of the system through its life cycle [adapted from ISO/IEC/IEEE 15288–2008].<br>*Note 1:* Stages relate to major progress and achievement milestones of the entity through its life cycle.<br>*Note 2:* Stages may be overlapping. |
| Operational Environment | Refer to *Environment of Operation*. |
| Operational Policies and Procedures | The security policies and procedures that address operations, maintenance, retirement, training, and the security-relevant aspects of other system-specific objective required to support the mission/business. |
| Operational Security Policy | A policy that addresses the operations, maintenance, retirement, training, and other security-relevant policy concerns associated with the system. |
| Organization | An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements) [NIST SP 800-53]. |
| Penetration Testing | A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system [NIST SP 800-53A]. |
| Policy Decision Point | A trusted human or technology entity that makes a policy-based decision in response to a request to perform some action. |
| Policy Enforcement Point | A trusted human or technology entity that carries out or enforces the decision made by the policy decision point. |
| Principle of Least Privilege | A foundational security principle that states that every program and every user of the system should operate using the least set of privileges necessary to complete the job. Primarily, this principle limits the damage that can result from an accident or error. It also reduces the number of potential interactions among privileged programs to the minimum for correct operation, so that unwanted, unintentional, or improper uses of privilege are less likely to occur. |
| Protection Needs | Informal statement or expression of the stakeholder security requirements focused on protecting information, systems, and services associated with mission/business functions throughout the system life cycle.<br>*Note:* Requirements elicitation and security analyses transform the protection needs into a formalized statement of stakeholder security requirements that are managed as part of the validated stakeholder requirements baseline. |

| | |
|---|---|
| Requirement | A condition or capability that must be met or possessed by a system or system element to satisfy a contract, standard, specification or other formally imposed documents [adapted from IEEE 610.12-1990].<br>Refer to *Requirements Baseline, Stakeholder Requirements, Stakeholder Requirements Baseline, Stakeholder Security Requirements, System Requirements, System Security Requirements*. |
| Requirements Baseline | The composite set of requirements at any time in the system life cycle which represent the agreed-to and approved set of requirements which serve to guide design and management decision processes [IEEE P1220]. |
| Requirements Traceability Matrix | A matrix that records the relationship between a set of requirements and one or more products of the development process and that is used to demonstrate completeness and coverage of an activity or analysis that is based upon the requirements contained in the matrix [adapted from IEEE Std 610.12-1990].<br>*Note:* The matrix may be a set of matrices representing requirements at different levels of decomposition. Such a traceability matrix enables the tracing of requirements stated in their most abstract form (e.g., statement of stakeholder requirements) through decomposition steps that result in the implementation that satisfies the requirements.<br>Refer to *Traceability Matrix.* |
| Risk | A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence [CNSSI 4009].<br>Security risk or security-relevant risk is that risk associated with the loss or degradation of confidentiality, integrity, or availability of assets.<br>*Note:* Information system-related security risks are risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Adverse impacts to the Nation include compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security [CNSSI 4009]. |

| | |
|---|---|
| Risk Assessment | The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system [NIST SP 800-39, NIST SP 800-37].<br>*Note:* Organizational risk encompasses the totality of risk concerns as defined by the stakeholders. The scope of a risk assessment is not limited to security-relevant concerns. Security risk assessment is one of multiple focused risk assessments that combine to ascertain risk to an organization and that are necessary to make risk-based trade-off decisions resulting from conflicting and competing mission/business needs.<br>Refer to *Security Risk Assessment.* |
| Risk Management | The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation or use of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system; and (iv) documenting the overall risk management program [CNSSI 4009]. |
| Risk Tolerance | The organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives [ISO 73].<br>*Note 1:* Risk tolerance can be influenced by legal or regulatory requirements [ISO Guide 73].<br>*Note 2:* Risk tolerance is the level of risk or degree of uncertainty that is acceptable to organizations and is the key element of the organizational risk frame [NIST SP 800-39]. |
| Risk Treatment | The process to modify risk.<br>*Note 1:* Risk treatment can involve: (i) avoiding the risk by deciding not to start or continue with the activity that gave rise to the risk; (ii) taking or increasing risk in order to pursue an opportunity; (iii) removing the risk source; (iv) changing the likelihood; (v) changing the consequences; (vi) sharing the risk with another party or parties (including contracts and risk financing); and (vii) retaining the risk by informed decision.<br>*Note 2:* Risk treatments that deal with negative consequences are sometime referred to as risk mitigation, risk elimination, risk prevention, or risk reduction.<br>*Note 3:* Risk treatment can create new risks or modify existing risks [ISO Guide 73]. |

| | |
|---|---|
| Security | A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protection measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach [CNSSI 4009].<br>*Note 1:* The CNSSI 4009 definition focuses on security as an organizational enterprise objective.<br>*Note 2:* The engineering perspective views security as a complex quality factor that is composed of multiple quality sub-factors. The most prevalent sub-factors are confidentiality, integrity, and availability. Additionally, the integrity sub-factor can be further divided into hardware, software, data, and communications integrity. Other security-relevant quality sub-factors include, but are not limited to, privacy and non-repudiation. There are also quality sub-factors that generally have been considered only by the system safety engineering, such as continuity, resiliency, and fault-tolerance, that are now being assessed in terms of susceptibility to malicious intent and the resultant impact on the mission/business; all motivated by mission assurance concerns that span the entire spectrum of incidental and accidental misuse through to attack by an advanced persistent threat.<br>The systems security engineering perspective ensures that all security-relevant quality sub-factors are satisfied by the engineered system and that the system achieves mission/business security objectives such as that defined by CNSSI 4009. |
| Security Architecture | A set of physical and logical security-relevant representations (i.e., views) of system architecture that conveys information about how the system is partitioned into security domains and makes use of security-relevant elements to enforce security policies within and between security domains based on how data and information must be protected.<br>*Note:* The security architecture reflects security domains, the placement of security-relevant elements within the security domains, the interconnections and trust relationships between the security-relevant elements, and the behavior and interactions between the security-relevant elements. The security architecture, like the system architecture, may be expressed at different levels of abstraction and with different scopes. |
| Security Concept of Operations (Security CONOP) | A security-focused description of an information system, its operational policies, classes of users, interactions between the system and its users, and the system's contribution to the operational mission [CNSSI 4009]. |
| Security Controls | The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information [CNSSI 4009]. |

| | |
|---|---|
| Security Domain | A set of users, rules, processes, systems, and services whose behavior and interactions are governed by a common security policy. A domain that implements a security policy and is administered by a single authority [CNSSI 4009]. |
| Security Function | The capability provided by a system element. The capability may be expressed generally as a concept or specified precisely in requirements. A security function must be implemented.<br>The hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based [NIST SP 800-53].<br>Refer to *Security Mechanism.* |
| Security Mechanism | A method, tool, or procedure for enforcing a security policy.<br>A security mechanism is the implementation of a concept or specified function.<br>Refer to *Security Function.* |
| Security Policy | A set of rules that govern security-relevant behavior. The rules can be stated at very high levels (e.g., an organizational policy defines acceptable behavior of employees in performing their mission/business functions) or at very low levels (e.g., an operating system policy that defines acceptable behavior of executing processes and their use of resources).<br>Refer to *Operational Security Policy*. |
| Security Relevance | Term used to describe those functions/mechanisms that are relied upon, directly or indirectly, to enforce security policy that governs confidentiality, integrity, and availability protections.<br>*Note:* The concept of security relevance is a continuum that represents the relationship between a function or mechanism and its significance (i.e., role, importance, and impact) in the enforcement of security policy. This continuum, in order of greatest to least significance, can be expressed as the following three types: (i) security-enforcing functions that are directly responsible for making or enforcing security policy decisions; (ii) security-supporting functions that contribute to the ability of security-enforcing functions to make or enforce security policy decisions; and (iii) security non-interfering functions that do not enforce or support any aspect of the security policy, but have the potential to adversely affect the correct operation of the security-enforcing and security-supporting functions. These functions must be understood to ensure that they are non-interfering. |
| Security Requirements | Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted [CNSSI-4009]. |

| | |
|---|---|
| Security Risk Assessment | Process and associated techniques to identify: (i) threats to the operations, information, systems, assets, and individuals of the organization; (ii) vulnerabilities associated with the operations, information, systems, assets, and individuals associated with the organization; (iii) consequences/impact to the mission/business should a threat successfully exploit a vulnerability; and (iv) the likelihood that a specific vulnerability will be exploited and a threat will be realized.<br>Refer to *Risk Assessment*. |
| Security Service | A capability that supports one or more of the security requirements (confidentiality, integrity, availability). Examples of security services are key management, access control, and authentication [CNSSI-4009]. |
| Security Specification | The requirements for the security-relevant portion of the system.<br>Detailed description of the safeguards required to protect an information system [CNSSI-4009].<br>*Note:* The security specification may be provided as a separate document or may be captured with a broader specification. |
| Sensitivity | A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection [CNSSI 4009]. |
| Service | A capability or function provided by an entity.<br>A mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description [OASIS SOA]. |
| Specification | A document that specifies, in a complete, precise, verifiable manner, the requirements, design, behavior, or other characteristics of a system or component and often the procedures for determining whether these provisions have been satisfied [IEEE Std 610.12-1990].<br>Refer to *Security Specification*. |
| Stakeholder | A person, group, or organization that has a legitimate direct or indirect interest in a system because that person, group, or organization can affect or be affected by the system's objectives, policies, or operations in any stage of the system life cycle.<br>*Note 1:* There is no definitive statement of stakeholder titles, roles, and responsibilities. Each engineering effort has its own set of stakeholders.<br>*Note 2:* An individual may be designated as the representative for a large group of stakeholders (e.g., user representative).<br>*Note 3:* The identity, role, and responsibility of stakeholders may change during the course of the systems engineering effort and as the system progresses through the stages of its life cycle. |

| | |
|---|---|
| Stakeholder Requirements | Requirements that specify stakeholder operational, protection, safety, and other needs, expectations, and constraints for systems to support the mission/business. The stakeholder requirements are formalized by the systems engineering team as part of the requirements elicitation process and presented to the stakeholders for validation.<br>Refer to *Validated Stakeholders Requirements Baseline.* |
| Stakeholder Security Requirements | The security-relevant stakeholder requirements. Stakeholder security requirements specify: (i) the protection needed for mission/business information, processes, functions, and systems; (ii) the roles, responsibilities, and security-relevant actions of individuals that perform and support the mission/business processes; (iii) the interactions between the security-relevant system elements; and (iv) the assurance that is to be obtained in the system.<br>Refer to *Security Requirements*. |
| Strength of Function | Criterion expressing the minimum efforts assumed necessary to defeat the specified security behavior of an implemented security function by directly attacking its underlying security mechanisms.<br>*Note 1:* Strength of function has as a prerequisite that assumes that the underlying security mechanisms are correctly implemented. The concept of strength of functions may be equally applied to services or other capability-based abstraction provided by security mechanisms.<br>*Note 2:* The term robustness combines the concepts of assurance of correct implementation with strength of function to provide finer granularity in determining the trustworthiness of a system. |
| System | A combination of interacting elements organized to achieve one or more stated purposes [ISO/IEC/IEEE 15288:2008].<br>*Note 1:* The term system, as used in this document, refers to those systems that process, store, and transmit data to provide a service or function, or to monitor and control physical devices, other systems, or capabilities. Examples of these systems include: general and special-purpose information systems; command, control, and communication systems; crypto modules; central processing unit and graphics processor boards; process control systems; flight control systems; weapons, targeting, and fire control systems; medical devices and treatment systems; financial, banking, and merchandising transactions systems; and social networking systems.<br>*Note 2:* This document uses the term information system in addition to system. Systems engineering focuses on all types of systems, including information systems (i.e., a type of system). As a specialty engineering field of systems engineering, systems security engineering must have that same focus. In this document, when the term information system is used, the intended meaning is any type of system. |

| | |
|---|---|
| System Context | The specific system elements, boundaries, interconnections, interactions, and environment of operation that define a system. |
| System Element | Member of a set of elements that constitutes a system.<br>*Note:* A system element is a discrete part of a system that can be implemented to fulfill specified requirements. A system element can be a discrete component, product, service, infrastructure, system, or enterprise. A system element can be implemented by hardware, software, data, humans, processes (e.g., processes for providing service to users), procedures (e.g., operator instructions), facilities, materials, and naturally occurring entities (e.g., water, organisms, minerals), or any combination [ISO/IEC/IEEE 15288:2008].<br>*Note:* Each system element may be a system. The recursive nature of the term system element conveniently allows the term system to apply equally when referring to a discrete component or a large, complex, and geographically distributed system of systems. |
| System Life Cycle | The period of time that begins when a system is conceived and ends when the system is no longer available for use [IEEE 610.12-1990].<br>The stages through which a system passes, typically characterized as initiation, development, operation, and termination (i.e., sanitization, disposal and/or destruction).<br>Evolution of a system, product, service, project or other human-made entity from conception through retirement [ISO/IEC/IEEE 15288:2008].<br>Refer to *Life Cycle Stages*. |
| System Security Requirements | System requirements that have security relevance. They define the protection capabilities provided by the system, the performance and behavioral characteristics exhibited by the system, and the evidence used to determine that the system security requirements have been satisfied.<br>*Note:* Each system security requirement is expressed in a manner that makes verification possible via analysis, observation, test, inspection, measurement, or other defined and achievable means.<br>Refer to *Security Requirement*. |
| System-of-Interest | The system that is the focus of the systems engineering effort. The system-of-interest contains system elements, system element interconnections, and the environment in which they are placed.<br>*Note 1:* The system-of-interest is an element of the system.<br>*Note 2:* The boundary of the system-of-interest is typically determined relative to the authorization boundary. However, it can be determined by other boundaries established by programmatic, operational, or jurisdictional control.<br>*Note 3:* The target system is also referred to as the system of interest. |

| | |
|---|---|
| System-of-Systems | A set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities.<br>System-of-interest whose system elements are themselves systems; typically these entire large-scale interdisciplinary problems with multiple, heterogeneous, distributed systems [INCOSE Handbook]. |
| Systems Engineering | Systems engineering is an engineering discipline whose responsibility is creating and executing an interdisciplinary process to ensure that the customer and all other stakeholder needs are satisfied in a high-quality, trustworthy, cost-efficient, and schedule-compliant manner throughout a system's entire life cycle [INCOSE Consensus of Fellows]. |
| Systems Security Engineer | Individuals that perform any or all of the activities defined by the systems security engineering process, regardless of their formal title. Additionally, the term systems security engineer refers to an individual or multiple individuals operating on the same team or cooperating teams. |
| Systems Security Engineering | Systems security engineering is a specialty engineering field strongly related to systems engineering. It applies scientific, engineering, and information assurance principles to deliver trustworthy systems that satisfy stakeholder requirements within their established risk tolerance. |
| Threat | Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service [CNSSI 4009]. |
| Threat Analysis | *Refer to Threat Assessment*. |
| Threat Assessment | Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat [CNSSI 4009]. |
| Traceability Analysis | The analysis of the relationships between two or more products of the development process conducted to determine that objectives have been met or that the effort represented by the products is completed.<br>*Note:* A requirements traceability analysis demonstrates that all system security requirements have been traced to and are justified by at least one stakeholder security requirement, and that each stakeholder security requirement is satisfied by at least one system security requirement. |
| Traceability Matrix | A matrix that records the relationship between two or more products of the development process (e.g., a matrix that records the relationship between the requirements and the design of a given software component) [IEEE Std 610.12-1990]. |

| | |
|---|---|
| Trade-off Analysis | Determining the effect of decreasing one or more key factors and simultaneously increasing one or more other key factors in a decision, design, or project.<br>Refer to *Architecture Trade-off Analysis Method*, *Design Trade-off Analysis*. |
| Trust | Trust is the belief that an entity will behave in a predictable manner while performing specific functions in specific conditions or circumstances.<br>Trust, from the security perspective, is the belief that a security-relevant entity will behave in a predictable manner while enforcing security policy.<br>*Note:* Trust is typically expressed as a range (e.g., levels or degrees) that reflects the measure of trustworthiness associated with the entity.<br>Refer to *Trustworthiness*. |
| Trust Relationship | An agreed-to relationship between two or more entities that is governed by a policy for communicating and protecting shared information and resources.<br>*Note:* This refers to trust relationships between technology system elements implemented by hardware, firmware, and software. |
| Trustworthiness | Trustworthiness is an attribute associated with an entity that reflects confidence that the entity will meet its requirements.<br>Trustworthiness, from the security perspective, reflects confidence that an entity will meet its security requirements while subjected to disruptions, human errors, and purposeful attacks that may occur in the environments of operation.<br>The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities [CNSSI 4009]. |
| Validated Stakeholder Requirements Baseline | Stakeholder requirements that are validated by the stakeholders and used by the systems engineering team to specify and develop the system to be delivered. The validated stakeholder requirements baseline is placed under configuration control and changes to the baseline are managed by a configuration management process. |
| Validation | Confirmation, through the provision of objective evidence, that the requirements for a specific intended use of application have been fulfilled.<br>*Note:* Validation is the set of activities ensuring and gaining confidence that a system is able to accomplish its intended use, goals, and objectives (i.e., meet stakeholder requirements) in the intended operational environment [ISO/IEC/IEEE 15288:2008, ISO 9000:2005]. |

| | |
|---|---|
| Verification | Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome) [CNSSI-4009].<br>*Note:* Verification is a set of activities that compares a system or system element against the required characteristics. This may include, but is not limited to, specified requirements, design description, and the system itself [ISO/IEC/IEEE 15288:2008, ISO 9000:2005].<br>Refer to *Independent Verification and Validation, Verification and Validation*. |
| Verification and Validation | The process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and the final system or component complies with specified requirements [IEEE Std 610.12-1990]. |
| Vulnerability | Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source [CNSSI 4009]. |
| Vulnerability Assessment | Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation [CNSSI 4009]. |

APPENDIX C

# ACRONYMS

COMMON ABBREVIATIONS

| | |
|---|---|
| CC | Common Criteria |
| CNSS | Committee on National Security Systems |
| DoD | Department of Defense |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronic Engineers |
| INCOSE | International Council on Systems Engineering |
| INFOSEC | Information Security |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| IV&V | Independent Verification and Validation |
| NIST | National Institute of Standards and Technology |
| OASIS | Advancing Open Standards for Information Systems |
| RMF | Risk Management Framework |
| SFR | Security Functional Requirement |
| SOA | Service-Oriented Architecture |
| SSE | Systems Security Engineering |
| V&V | Verification and Validation |

APPENDIX D

# SUMMARY OF ACTIVITIES AND TASKS

SYSTEMS SECURITY ENGINEERING PROCESSES, ACTIVITIES, AND TASKS

| TECHNICAL PROCESSES | |
|---|---|
| **SR** | **Stakeholder Requirements Definition Process** |
| SR-1 | ELICIT STAKEHOLDER SECURITY REQUIREMENTS |
| SR-1-1 | Identify the stakeholders who have an interest in or are responsible for the protection of the system throughout its life cycle. |
| SR-1-2 | Elicit stakeholder security requirements from the identified stakeholders with protection interests or responsibilities related to the system. |
| SR-2 | DEFINE STAKEHOLDER SECURITY REQUIREMENTS |
| SR-2-1 | Define the security-relevant constraints on the system. |
| SR-2-2 | Identify the interaction between users and the system including any services required for the operational support of the system. |
| SR-2-3 | Identify and assess threats to mission/business assets. |
| SR-2-4 | Determine mission/business asset protection needs. |
| SR-2-5 | Specify the stakeholder security requirements and identify the functions that relate to the mission/business protection needs of the stakeholders. |
| SR-3 | ANALYZE AND MAINTAIN STAKEHOLDER SECURITY REQUIREMENTS |
| SR-3-1 | Analyze the stakeholder security requirements. |
| SR-3-2 | Resolve any conflicts, inconsistencies, or gaps in the stakeholder security requirements. |
| SR-3-3 | Convey stakeholder security requirements to stakeholders to ensure that their protection needs and expectations have been adequately captured and expressed. |
| SR-3-4 | Record and maintain stakeholder security requirements in a form suitable for requirements management throughout the system life cycle. |
| **RA** | **Requirements Analysis Process** |
| RA-1 | DEFINE SYSTEM SECURITY REQUIREMENTS |
| RA-1-1 | Define the security functional boundary, security domains, trust domains, and context of the system in terms of the security behavior and properties to be provided. |
| RA-1-2 | Define each security function that the system is required to perform and develop the security concept of operations for the intended use of the security functions of the system. |
| RA-1-3 | Define necessary implementation constraints including: (i) constraints that are introduced by the stakeholder requirements or that are unavoidable security solution limitations; and (ii) constraints that are imposed by the system security requirements on the system requirements or that are unavoidable solution limitations imposed by the system security requirements. |
| RA-1-4 | Define technical and quality in use measures that enable the assessment of technical achievement. |

| | |
|---|---|
| RA-1-5 | Define system security requirements. |
| RA-1-6 | Determine the responsibility for system security requirement satisfaction. |
| RA-2 | ANALYZE AND MAINTAIN SYSTEM SECURITY REQUIREMENTS |
| RA-2-1 | Analyze the integrity and effectiveness of the system security requirements. |
| RA-2-2 | Convey the analyzed system security requirements to the applicable stakeholders to ensure that the specified system security requirements adequately reflect the stakeholder security requirements and are sufficient to address their protection needs and protection expectations. |
| RA-2-3 | Demonstrate traceability between the system security requirements and the stakeholder security requirements. |
| RA-2-4 | Maintain the system security requirements and associated rationale, decisions, and assumptions throughout the system life cycle. |
| **AD** | **Architectural Design Process** |
| AD-1 | DEFINE THE SECURITY ARCHITECTURE |
| AD-1-1 | Define the logical security architectural design. |
| AD-1-2 | Partition the system security functions identified in requirements analysis, allocate those functions to elements of the system security architecture to achieve trust relationships, and generate derived security requirements that result from the allocations. |
| AD-1-3 | Define and document the security interfaces, security interconnections, and the trust relationships between system elements and between the system and external systems. |
| AD-2 | ANALYZE AND EVALUATE THE SECURITY ARCHITECTURE |
| AD-2-1 | Analyze the resulting security architectural design to establish security design criteria for each element. |
| AD-2-2 | Determine which system security requirements are allocated to authorized operators, maintainers, administrators, and other designated authorized users. |
| AD-2-3 | Determine whether existing infrastructures, services, and hardware/software elements that satisfy the security architectural design and interface criteria are available. |
| AD-2-4 | Evaluate alternative security architectural design solutions, modelling those solutions to a level of detail that permits comparison against the specifications expressed in the system security requirements and the assurance and trustworthiness, risk, performance, cost, and time scales expressed in the stakeholder security requirements. |
| AD-3 | DOCUMENT AND MAINTAIN THE SECURITY ARCHITECTURE |
| AD-3-1 | Specify the selected physical security design solution as a security architectural design baseline in terms of its functions, performance, behavior, interfaces, interconnections, trust relationships, security domains, and unavoidable implementation constraints. |
| AD-3-2 | Record the security architectural design information. |
| AD-3-3 | Maintain mutual traceability between specified design and system requirements. |
| **IP** | **Implementation Process** |
| IP-1 | PLAN THE SECURITY IMPLEMENTATION OF SYSTEM ELEMENTS |
| IP-1-1 | Generate a security implementation strategy for system elements. |
| IP-1-2 | Identify security constraints that the security implementation strategy and security implementation technology impose on security and non-security design solutions. |

| | |
|---|---|
| IP-2 | PERFORM SECURITY IMPLEMENTATION OF SYSTEM ELEMENTS |
| IP-2-1 | Realize or adapt system elements using the implementation-enabling systems and specified materials according to the defined security implementation procedures. |
| IP-2-2 | Record evidence that the system elements meet the security aspects of supplier agreements, legislation, and organizational policy. |
| IP-2-3 | Securely package, store, and distribute the system elements. |
| **IN** | **Integration Process** |
| IN-1 | PLAN THE SECURITY INTEGRATION OF SYSTEM ELEMENTS |
| IN-1-1 | Define an assembly sequence and strategy that minimizes system security integration time, costs, and risks. |
| IN-1-2 | Identify the security constraints on the architectural design resulting from the integration strategy. |
| IN-2 | PERFORM SECURITY INTEGRATION OF SYSTEM ELEMENTS |
| IN-2-1 | Obtain integration-enabling systems and specified materials according to the defined system integration procedures. |
| IN-2-2 | Obtain system elements in accordance with secure distribution considerations, requirements, and constraints documented in agreements. |
| IN-2-3 | Assure that the security-relevant system elements have been verified and validated against security acceptance criteria specified in an agreement. |
| IN-2-4 | Integrate security-relevant systems elements in accordance with applicable interface control descriptions and defined assembly procedures, using the specified integration facilities. |
| IN-2-5 | Analyze, record, and report security integration information, including results of security integration actions, nonconformance, and corrective actions taken. |
| **VE** | **Verification Process** |
| VE-1 | PLAN THE SECURITY VERIFICATION OF THE SYSTEM |
| VE-1-1 | Define the strategy for system life cycle verification of security-relevant system elements and system security. |
| VE-1-2 | Prepare a security verification plan based on system security requirements and assurance objectives. |
| VE-1-3 | Identify constraints on system and security design decisions that result from the security verification strategy and plan. |
| VE-2 | PERFORM SECURITY VERIFICATION OF THE SYSTEM |
| VE-2-1 | Ensure that the enabling systems, test suites, equipment, simulators, facilities, and operators used for security verification are available and prepared for the verification of security-relevant system elements. |
| VE-2-2 | Conduct security verification to demonstrate that: (i) system security requirements and security architectural design are satisfied; (ii) security protections are continuous in all defined modes of system operation; (iii) the system is sufficiently resistant to attack and misuse; and (iv) sufficient evidence exists to demonstrate achievement of trustworthiness objectives. |
| VE-2-3 | Conduct a vulnerability assessment to identify exploitable vulnerabilities and vulnerabilities that may be triggered by errors of omission, commission, or by system faults and failures. |
| VE-2-4 | Conduct penetration testing to identify methods by which vulnerabilities may be intentionally exploited or unintentionally triggered. |
| VE-2-5 | Conduct misuse testing to identify methods by which the system can be used as specified to produce unspecified emergent behavior that does not conform to security requirements. |

| | |
|---|---|
| VE-2-6 | Provide and protect system verification data in accordance with agreements and legal or regulatory requirements. |
| VE-2-7 | Analyze, record, and report security verification, discrepancy, and corrective action information. |
| **TR** | **Transition Process** |
| TR-1 | PLAN FOR THE SECURE TRANSITION OF THE SYSTEM |
| TR-1-1 | Prepare the strategy for secure transition of the system. |
| TR-1-2 | Prepare the site of operation in accordance with installation security requirements, directives, policies, procedures, regulations, and local/site ordinances. |
| TR-2 | PERFORM THE SECURE TRANSITION OF THE SYSTEM |
| TR-2-1 | Deliver the system for installation at the specified location and time in accordance with the security measures described in the transition strategy. |
| TR-2-2 | Install the system at its specified location and establish the interconnections that constitute trust relationships to its environment of operation in accordance with the system security specification and the security measures described in the transition strategy. |
| TR-2-3 | Demonstrate proper installation, generation, configuration, and start-up of the system in accordance with the system security specification and security acceptance testing. |
| TR-2-4 | Demonstrate that the installed system and its enabling systems are capable of delivering the required security services using the results of security acceptance tests, vulnerability assessments, penetration testing, and as specified in agreements. |
| TR-2-5 | Analyze, record, and report the security transition information, including results of security transition actions, nonconformance, and corrective actions taken. |
| **VA** | **Validation Process** |
| VA-1 | PLAN THE SECURITY VALIDATION OF THE SYSTEM |
| VA-1-1 | Define the strategy for validating the end-to-end security protections and security services in the operational environment and for achieving stakeholder security satisfaction. |
| VA-1-2 | Define a security validation plan based on stakeholder security requirements. |
| VA-2 | PERFORM SECURITY VALIDATION OF THE SYSTEM |
| VA-2-1 | Ensure that the enabling systems, test suites, equipment, simulators, facilities, and personnel used for security validation are available and prepared to conduct the validation. |
| VA-2-2 | Conduct security validation to demonstrate that the system protections conform to stakeholder security requirements and are effective given the mission/business concept of operation and the intended use of the system. |
| VA-2-3 | Conduct a vulnerability assessment to identify exploitable vulnerabilities and vulnerabilities that may be triggered by errors of omission, commission, or by system faults and failures. |
| VA-2-4 | Conduct penetration testing to identify exploitable vulnerabilities and to determine the residual susceptibility to specific malicious threat events. |
| VA-2-5 | Conduct misuse testing to identify methods by which the system can be used as specified but results in a violation of security policy or unspecified system behavior. |
| VA-2-6 | Make available security validation data on the system and obtain stakeholder concurrence. |
| VA-2-7 | Analyze, record, and report security validation information in accordance with the criteria defined in the security validation plan. |

| **OP** | **Operation Process** |
|---|---|
| OP-1 | PREPARE FOR THE SECURE OPERATION OF THE SYSTEM |
| OP-1-1 | Prepare a strategy for secure operation of the system. |
| OP-1-2 | Obtain other services related to the secure operation of the system. |
| OP-1-3 | Establish criteria to train and qualify personnel to securely operate the system. |
| OP-2 | PERFORM SECURITY OPERATIONAL ACTIVATION OF THE SYSTEM |
| OP-2-1 | Activate the system in its environment of operation to deliver secure services in accordance with the intended purpose of the system. |
| OP-2-2 | Verify that the system is operating as specified. |
| OP-3 | USE THE SYSTEM TO SECURE OPERATIONS |
| OP-3-1 | Monitor system operations to ensure that the system: (i) is being used in accordance with its stated purpose; (ii) is being operated in a secure manner consistent with the security concept of operations; and (iii) is compliant with security- and privacy-relevant legislation, Executive Orders, directives, regulations, policies, and procedures. |
| OP-3-2 | Monitor system operations to confirm that service performance is within acceptable security parameters and to detect vulnerabilities. |
| OP-3-3 | Monitor system operations to detect adversarial activity. |
| OP-4 | PERFORM OPERATIONAL SECURITY PROBLEM RESOLUTION |
| OP-4-1 | Identify security failures that affect the delivery of system services or the conduct of secure system operations. |
| OP-4-2 | Determine the appropriate course of action to respond to a security failure and implement remediation. |
| OP-5 | SUPPORT THE CUSTOMER TO PROVIDE CONTINUOUS PROTECTION OF ASSETS |
| OP-5-1 | Establish a mechanism for continuous communication with stakeholders and improvement in the security-relevant aspects of the system. |
| **MA** | **Maintenance Process** |
| MA-1 | PLAN FOR THE SECURE MAINTENANCE OF THE SYSTEM |
| MA-1-1 | Prepare a strategy for the secure maintenance of the system. |
| MA-1-2 | Determine the security criteria for system maintenance tools. |
| MA-1-3 | Determine the security qualification for maintenance personnel. |
| MA-2 | PERFORM SECURE MAINTENANCE ON THE SYSTEM |
| MA-2-1 | Conduct system maintenance in accordance with the secure maintenance strategy. |
| MA-2-2 | Initiate corrective security action to remedy previously undetected security design errors and oversights. |
| MA-2-3 | Document security-relevant maintenance activities, the need for corrective action, and the corrective action that was performed. |
| **DS** | **Disposal Process** |
| DS-1 | PLAN FOR THE SECURE DISPOSAL OF THE SYSTEM |

| | |
|---|---|
| DS-1-1 | Prepare a strategy for the secure disposal of the system, to include each system element, system and stakeholder material, data, and information assets. |
| DS-1-2 | Define the constraints on system requirements and system design that are unavoidable consequences of the secure disposal strategy. |
| DS-1-3 | Specify secure storage criteria for the elements of the system, mission/business assets, and system assets to be stored. |
| DS-2 | PERFORM SECURE DISPOSAL OF THE SYSTEM |
| DS-2-1 | Acquire the enabling systems or services to be used during secure disposal of a system. |
| DS-2-2 | Deactivate the system to prepare it for secure removal from operation. |
| DS-2-3 | Conduct security debriefings, revoke authorizations for access to sensitive system material and information assets, and collect all sensitive data, information, and material assets from system user, operations, maintenance, and support personnel. |
| DS-2-4 | Sanitize security-relevant system elements prior to disposal, release out of organizational control, or release for reuse. |
| DS-2-5 | Ensure appropriate protections are in place for system components, data, and information during removal, reuse, recycling, reconditioning, overhaul, or destruction. |
| DS-2-6 | Verify that all identified sensitive material and information assets have been accounted for and have been properly disposed of, stored, or placed in a new environment of operation. |
| DS-2-7 | Verify that all archived information has sufficient security and privacy protections in place, to include periodic reviews and audits to determine when protections are no longer required or when the archived information may be securely destroyed. |

APPENDIX E

# INFORMATION SECURITY RISK MANAGEMENT

DEFINING THE RELATIONSHIP TO SYSTEMS SECURITY ENGINEERING PROCESSES

[Note: The contents of this appendix will address the integration of the current information security risk management process (including the Risk Management Framework [RMF], security controls, and other security- and risk-related concepts), into the systems security engineering processes. In particular, the appendix will describe how the information security risk management concepts contained in the *Unified Information Security Framework*, including Joint Task Force publications SP 800-30, SP 800-37, SP 800-39, SP 800-53, and SP 800-53A, can be effectively applied to the security-enhanced systems engineering processes defined in Chapter Three.[68] This appendix will be released for public review separately from the main publication and will be added to the publication prior to the final public draft.]

[68] *Information security risk management* concepts will also be addressed in some of the nontechnical systems security engineering processes, including for example, the security-enhanced ISO/IEC/IEEE 15288 *Risk Management* process, to be published in subsequent drafts of this document.

APPENDIX F

# USE CASE SCENARIOS

APPLYING SYSTEMS SECURITY ENGINEERING TO SYSTEM ENGINEERING PROCESSES

[Note: The contents of this appendix will contain use case scenarios to provide examples of how to apply systems security engineering to the systems engineering processes throughout the system life cycle in order to deliver systems under different circumstances and subject to varying constraints. This appendix will be released for public review separately from the main publication and will be added to the publication prior to the final public draft.]

APPENDIX G

# ROLES AND RESPONSIBILITIES

SYSTEMS SECURITY ENGINEERING ROLES AND RESPONSIBIITIES

[Note: The contents of this appendix will describe the various roles and responsibilities associated with carrying out the systems security engineering processes during all stages of the system life cycle. This appendix will be released for public review separately from the main publication and will be added to the publication prior to the final public draft.]

APPENDIX H

# SECURITY AND TRUSTWORTHINESS

DEFINING THE FUNDAMENTAL PRINCIPLES OF SECURITY AND TRUSTWORTHINESS

[Note: The contents of this appendix will provide a comprehensive tutorial of the fundamentals of security and trustworthiness that serve as a basis for systems security engineering activities, the conduct of those activities, and for the outcomes produced by those activities. This appendix will be released for public review separately from the main publication and will be added to the publication prior to the final public draft.]

APPENDIX I

# SYSTEM RESILIENCY

INTEGRATING RESILIENCY TECHNIQUES INTO THE SYSTEMS ENGINEERING PROCESS

[Note: The contents of this appendix will address the concept of *systems resiliency* and how well-executed systems security engineering processes can contribute to delivering systems that by design and through rigorous development techniques are inherently more resilient and capable of continued operation in the face ongoing threats, including for example, cyber attacks and structural/component failures. This appendix will be released for public review separately from the main publication and will be added to the publication prior to the final public draft.]

APPENDIX J

# DEPARTMENT OF DEFENSE ENGINEERING PROCESS

DOD APPLICATION OF THE SYSTEMS SECURITY ENGINEERING PROCESS

[Note: The contents of this appendix will contain specific systems security engineering guidance for U.S. Department of Defense Programs. This appendix will be released for public review separately from the main publication and will be added to the publication prior to the final public draft.]

APPENDIX K

# ACQUISITION CONSIDERATIONS

SYSTEMS SECURITY ENGINEERING IN THE ACQUISITION PROCESS

[Note: The contents of this appendix will address how organizations can: (i) acquire systems security engineering services to perform the activities and tasks described in Chapter Three; or (ii) specify that systems security engineering be accomplished when acquiring and integrating any IT product, system, or service. This appendix will be released for public review separately from the main publication and will be added to the publication prior to the final public draft.]