



The Cybersecurity Think Tank

NIST SP 800-160:

For the Rest of Us

An ICIT Summary

May 2016

Author

Drew Spaniel (ICIT Visiting Scholar, Carnegie Mellon University)

Contents

Introduction:	4
Chapter 1:.....	6
Chapter 2:.....	8
Chapter 3:.....	8
Agreement Processes:	10
Acquisition Process (AQ):.....	10
Supply Process (SP):	10
Organizational Project-Enabling Processes:.....	10
Life Cycle Model Management (LM):.....	10
Infrastructure Management (IF):	11
Portfolio Management (PM):.....	11
Human Resources Management (HR):.....	11
Quality Management (QM):.....	12
Knowledge Management (KM):	12
Technical Management Processes:.....	12
Project Planning (PL):	12
Project Assessment and Control (PA):	13
Decision Management (DM):.....	13
Risk Management (RM):	14
Configuration Management (CM):.....	14
Information Management (IM):.....	15
Measurement (MS):.....	15
Quality Assurance (QA):	16
Technical Processes:	16
Business or Mission Analysis Process (BA):.....	16
Stakeholder Needs and Requirements Definition Process (SN):	16
System Requirements Definition Process (SR):.....	17
Architecture Definition Process (AR):	18

Design Definition Process (DE):.....	19
System Analysis Process (SA):	19
Implementation Process (IP):.....	20
Integration Process (IN):	20
Verification Process (VE):	20
Transition Process (TR):	21
Validation Process (VA):.....	21
Operation Process (OP):.....	22
Maintenance Process (MA):.....	22
Disposal Process (DS):	23
Conclusion:	24

Introduction:

The days of Security Theater and organizations squeaking by via the illusion of cyber defense are over. Highly organized and hyper evolved adversaries assault and successfully breach our virtually defenseless IoT perimeters, networks, devices and virtually anything attached to each organization's technical microcosm. A new standard for critical infrastructure cybersecurity is a mandatory prerequisite to viable defense. SP 800-160 offers useful strategies that can raise the bar for cyber defense and can be implemented quickly to drastically minimize traditionally vulnerable attack surfaces laid siege by state sponsored APTs, hackers, sophisticated mercenaries and cyber jihad hackers. The threats are real, most networks are vulnerable and adversaries are consistently devising exploits that render devastating impact to targets.

This condensed review of SP 800 – 160 is meant to assist those who are new to this arena and want to delve into the useful strategies the full report possesses but may be limited in comprehension of technical jargon and industry vernacular. This version does not replace the full value of the original document authored by NIST; rather it can be considered a simplified and quick reference guide in a more consolidated format.

The economic stability and national security of the United States is dependent upon immensely powerful and intricately complex information systems, which are susceptible to a multitude of incidents due to a lack of a formalized framework for the development of engineering based solutions that are capable of addressing the “growing complexity, dynamicity, and interconnectedness of today's systems.” Information systems are vulnerable to the machinations of malicious cyber-adversaries, to the effects of natural disasters, to the misfortune of structural or component failures, and to errors of omission and commission. The complete dependence of the public and private sector upon foundationally insecure systems jeopardizes the mission and business success of individual organizations and it jeopardizes the stability of the United States as a nation. After decades of constructing systems without incorporating security through the life cycle of the system, the United States is underprepared for the threats that arose in the age of information. According to the conclusion of the January 2013 Defense Science Board Task Force Report entitled *Resilient Military Systems and the Advanced Cyber Threat*, “...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 colloquial definition of insanity is doing the same thing over and over and expecting a different result. Scientifically speaking, nothing changes without an application of will and force. The incessant barrage of cyber-attacks, service disruptions, and critical failures experienced by every level of government, the military, the private sector, critical infrastructure facilities, and private individuals, confirms the notion that adhering to the same old information security practices will not alter the inevitable result. In

order for different results to materialize, we must adjust our approach to the development of information security systems. According to NIST Sr. Fellow Dr. Ron Ross, fundamentally changing system security culture will require “a substantial investment in the requirements, architecture, design, and development of systems, components, applications, and networks.” The modern approach to system security must include: an understanding of the threat landscape, an understanding of organizational assets and the capability to protect those assets according to their criticality to the mission, an understanding of the increasingly complexity of systems and systems-of-systems, an understanding of how to incorporate information security requirements, functions, and services into established managerial and technical processes within organizations, and an understanding of how the trust and the security of a system can be better assured through measurable and repeatable processes. These understandings will inform a disciplined, structured, and standardized framework for system security engineering that is scientific and focused on the needs of the stakeholders.

As an organization of scientists, the National Institute for Standards and Technology (NIST) recognizes the necessity for improvement upon established best practices in order to address the modern threat landscape. In particular, NIST recognizes the need for trustworthy and secure systems that are dependable and resilient against compromise. Failure to adopt trustworthy and secure systems will leave the Nation susceptible to the potentially catastrophic consequences of complex incidents, such as serious natural disasters or cyber-warfare. As a result, NIST has released the second revision of Special Publication 800-160: **Systems Security Engineering: Consideration for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems** for public comment from May 4, 2016 through July 1, 2016. Assuring that a modern system is trusted requires a level of confidence in the conceptual framework, the development parameters, and the functionality, designed into a system from its inception through its lifecycle. In many ways, information security remains, at best, a soft science. NIST SP 800-160 introduces the rigor of the natural sciences to cybersecurity. The publication applies more methodical, Engineering-based approaches to information security solutions to address the dynamic, complex, and interconnected systems and systems-of-systems, such as the Internet of Things, that run the modern world. The level of trust that an organization can place in a system is dependent on how that system is expected to perform across a range of activities and how it actually performs in reality. The framework provided unites expectations, constraints, limitations, and uncertainties into security concerns and aids the user in addressing those concerns in a manner that builds confidence that the system will function as intended across the spectrum of disruptions, hazards, and threats.

NIST Special Publication 800-160 details the engineering-driven processes necessary to develop more defensible, resilient, and survivable systems. It aims to focus on imbuing trust and security in systems in consideration of the difficulties and challenges presented by reality through the implementation of a lifecycle driven, applied system engineering framework that is

built upon established standards and processes. In particular, NIST built the framework upon the holistic standards for systems and software engineering set forth by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the Institute for Electrical and Electronics Engineers (IEEE) and then it appended those processes with system security engineering techniques, methods, and practices. The predominant purpose of NIST SP 800-160 is to address information system security according to stakeholder requirements and protection needs and to “use established engineering processes to ensure that those requirements are addressed with the appropriate amount of fidelity and vigor, early and in a sustainable manner throughout the life cycle of the system.” NIST SP 800-160 has five main objectives. First, it aims to formalize a disciplined basis for security engineering in terms of principles, concepts, and activities. Next, it aims to promote a common security development mentality that applies to any system, regardless of its scope, size, complexity, or stage in the lifecycle. It aims to provide considerations and demonstrations of the ways that principles, concepts, and activities can be applied to the systems engineering process. NIST hopes that the special publication will foster growth in the application, study, and development of the field of systems engineering. Finally, NIST hopes that the framework will serve as a basis for educational and training initiatives that focus around individual certifications and professional assessment criteria.

Chapter 1:

Modern systems are unarguably more ubiquitous, more complex, and more interconnected than the systems upon which the foundations of information security were based. A more systematic security model is needed to promote trustworthiness, more than security, throughout the development life cycle of new systems. Security is a prediction of a system’s resiliency to compromise while trustworthiness is an estimate of a system component’s ability to perform its critical role under a variety of situations. Trustworthiness requirements could include attributes of safety, security, reliability, dependability, performance, resilience, and survivability under adversarial conditions such as attempts at disruption, natural disasters, or sophisticated threats. In terms of system security engineering, a trusted system is one that meets specific security requirements in addition to meeting other critical requirements. Without a new model, systems will continue to collapse due to malicious attacks, natural disasters, user errors, and other calamities because organizations will fail to alter their already failing security strategies to meet changes in the threat landscape. The inevitable breaches will result in major inconveniences and catastrophic losses for United States citizens.

A trust-driven model, such as that proposed in NIST SP 800-160, will preclude many breaches by removing vulnerabilities before adversaries can exploit them. In typical security models, information security is either predictive or reactive. In either case, information about the threat must be known before action can be taken. Trusted systems ignore that constraint. A

trusted system is not impervious to compromise; rather, it is developed from initiation to preclude vulnerabilities that result from design and to withstand attacks from a resourceful adversary. Having a greater level in trustworthiness of a system allows personnel to more effectively develop and implement incident response procedures. Security is reached when a system is free of risk and is completely trusted. NIST 800-160 uses a stakeholder driven model to engineer systematic trust and to aspire towards system security. To maximize the potential of the system security engineering model, security requirements for the protection of all mission and business critical assets must be defined and managed. In the NIST SP 800-160 framework, the role of security engineer applies to any information security or technical personnel who implements security controls according to the model in information systems. The security engineering model itself does not focus on what is likely to happen, as a traditional security model does. Instead, it prepares systems for what can happen. The model proactively prepares systems to prevent loss of an asset that the organization is not willing to accept. If compromise does occur, then the system is primed to minimize the consequence of the loss and to reactively respond to the loss.

The systems security engineering model applies to every system at every stage of the life cycle. Under the model, during the concept and development stages of the system life cycle, new systems are conceptually explored and then they are compared against alternatives. The results of the analysis and preliminary or applied research is used to refine the concept parameters and feasibility of the technologies applied within the system. The application of the engineering model to systems in operation, known as fielded systems, is designed to occur independently or concurrently with day-to-day operations, during the production, utilization, and/or support stages of the system lifecycle. Application of the model to fielded systems occurs as a result of adversity, such as disruptions, hazards, cyber-threats, incidents, errors, accidents, faults, component failures, and natural disasters that diminish or prevent the system from achieving its design intent. If, during the production, utilization, or support stages, the fielded system is upgraded to enhance existing capabilities while sustaining day-to-day operations, the model provides security considerations. If an organization wishes to upgrade a fielded system to result in a new system, then the model facilitates a framework in which upgrades are performed in a development environment that is independent of the fielded system. When necessary, the model provides an agile framework for transitioning a system from one operating environment or set of operating conditions to another operating environment or set of operating conditions. Arguably the greatest utility of the framework is its applicability to systems-of-systems (SoS) comprised of constituent systems that each have its own set of stakeholders, purpose, and planned evolution. Systems -of-systems, such as the Internet of Things, are created to produce a capability that would be impractical or impossible to achieve from a single constituent system. The framework applies to systems-of-systems across a continuum ranging from unplanned to a centrally managed engineering effort. Finally, the framework applies to systems entering the retirement phase of the life cycle. The model assists in the removal of functions, services, effects, and

dependencies from the operational environment to ensure that the entire system is removed (if desired). It also details the process to transition to a new system whose functions and services can replace those of the old system while sustaining day-to-day operations.

Chapter 2:

System Engineering is comprised of scientific, mathematic, engineering, and measurement principles, concepts, and methods, which are leveraged to increase the trust and reliability of a system. Systems Engineering is a collection of technical and non-technical processes, activities, and tasks that apply to various stages of the system life cycle. The technical processes ensure that the system meets critical quality metrics and that it meets stakeholder requirements through the application of engineering analysis and design principles. The nontechnical processes are used to manage aspects of the project, secure agreements between parties, and enable support to facilitate the project. “System engineering applies critical thinking to solve problems and balances the often-conflicting design constraints of operation and technical performance, cost, schedule, and effectiveness to optimize the solution, and to do so with an acceptable level of risk.” The technical and nontechnical processes must be institutionalized and operationally integrated into the organization, rather than kept disconnected from the traditional activities of the organization.

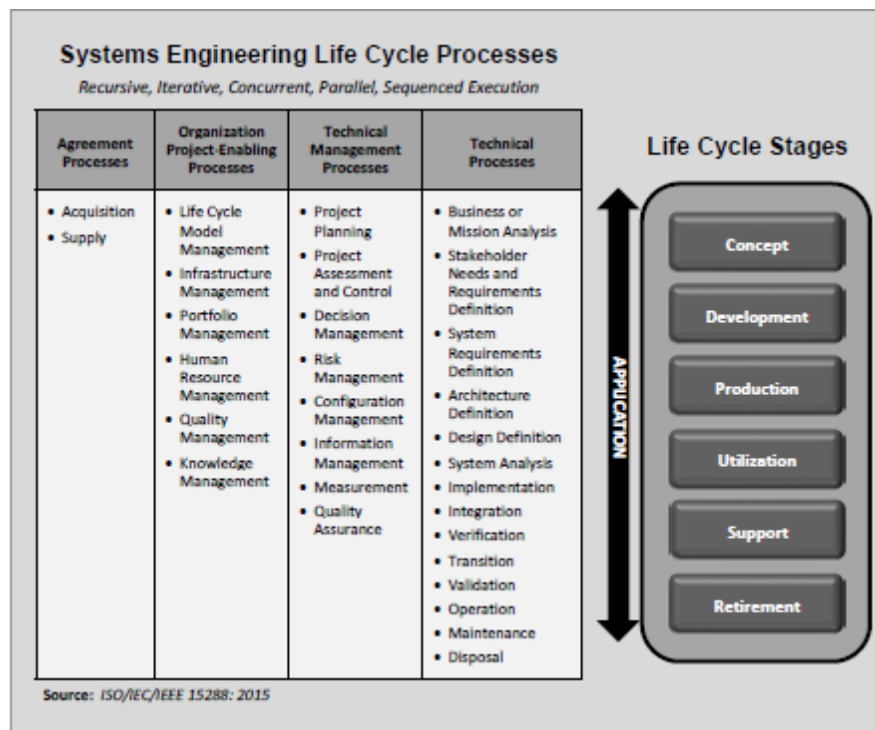
The model is built to be flexible and outcome-oriented, but it depends on close coordination between the system engineers and the stakeholders. The system engineering process does not end after a system is deployed, it continues throughout the life cycle of the system. In order for the model to succeed, the stakeholders responsible for utilization, support, and retirement of the system must continuously provide data and feedback to the system engineering team. The system developed does not need to be perfectly secure, but it does need to be adequately secure and trustworthy enough to address the stakeholders’ concerns related to the consequences associated with the loss of assets critical to the mission and purpose of the organization. “Adequately secure” is defined as freedom from the conditions that could cause the loss of assets with unacceptable consequences. The advantage of the system security model over a traditional security model is that it does not focus on the threat; instead, it focuses on mitigating and minimizing the consequences of the loss of critical assets.

Chapter 3:

Chapter three of NIST SP 800-160 covers the specific systems engineering processes that organizations can incorporate to add trust and security to their systems. The thirty system engineering processes are aligned and developed in conjunction with ISO/IEC/IEEE 15288. They are aligned into four families: Agreement Processes, Organization Project-Enabling Processes, Technical Management Processes, and Technical Processes. The activities and tasks

in each process are founded in security and trust principles and concepts and are designed to facilitate consistency in the model. The processes are not designed to be prescriptive controls; instead, they are designed “to be applied concurrently, iteratively, or recursively, at any level of the structural hierarchy of a system, with the appropriate fidelity and rigor, and at any stage in the system life cycle, in accordance with acquisition, system engineering, or other imposed models.” To provide flexibility and agility of design across a variety of systems and applications, the processes are designed to be tailored to their application.

Figure 1: System Engineering Processes and System Life Cycle



Agreement Processes:

Acquisition Process (AQ):

The *Acquisition* process is used to obtain a product or service from a supplier that meets the organization's security requirements and concerns. The organization should define the security aspects of its acquisition strategy and how the acquisition will be conducted. It should prepare a product or service request that clearly includes its security requirements and it should securely communicate that request to potential suppliers. It should begin negotiations with one or more suppliers who are capable of meeting the security criteria of the request. Agreements should be developed that specify that the supplier is capable and willing to satisfy the security criteria. The organization should evaluate the security impact of any necessary changes to the agreement prior to acceptance by both parties. The execution of the security aspects of the agreement should be regularly assessed. The delivered product or service should be regularly evaluated according to the security criteria specified in the agreement. If the product meets the agreed terms, then the acquirer should accept the product from the supplier according to the terms of the agreement. For a timely response, the acquirer should securely provide data to the supplier concerning issues.

Supply Process (SP):

The *Supply* process is used to provide an acquirer with a product or service that meets specific security requirements. The supplier should inspect the acquirer's request for a product or service and identify the security aspects therein. The supplier should define their own security aspects according to their supply strategy. The request should be considered with regard to the supplier's ability to satisfy the security criteria and the feasibility of the request. The supplier should prepare a response to the acquirer. They should develop an agreement containing the specific security aspects for a product and the security criteria that it will be measured against. They should recognize and evaluate the security impact of changes to the agreement and then negotiate any necessary changes with the acquirer. The security aspects of the agreement should be executed according to the engineering project plans. The execution of the security aspects of the agreement should be regularly assessed. The product should be delivered according to the terms of the agreement. If specified in the agreement, the supplier should provide security assistance to the acquirer upon request. If specified in the agreement, the supplier should transfer responsibility for the product or service to the acquirer or a third party.

Organizational Project-Enabling Processes:

Life Cycle Model Management (LM):

The *Life Cycle Model Management* process is used to define, maintain, and assure the availability of policies, life cycle processes, life cycle models, and procedures. The process begins with the establishment of the security-aligned policies and procedures for process management and deployment and security criteria for the standard life cycle models. The

organization should define the security aspects of the business criteria that control progression through the life cycle and the roles, responsibilities, and authorities necessary to facilitate incorporation of security aspects of processes and the strategic management of the life cycle. The security aspects of process execution should be monitored throughout the life cycle and periodically reviewed. The results should inform improvements and adjustments to the criteria. The organization should prioritize and plan for security improvement opportunities and it should inform stakeholders when it implements those opportunities.

Infrastructure Management (IF):

The *Infrastructure Management* process is used to support the organization by providing the infrastructure and services to support projects throughout the life cycle. The organization should define relevant security aspects and then identify, obtain, and provide the infrastructure resources that adequate security functionality to support projects. The degree to which delivered resources satisfy project protection needs should be regularly evaluated. The delivery of resources should adapt or change as project requirements change.

Portfolio Management (PM):

The *Portfolio Management* process is used to meet the strategic goals of the organization by initiating and sustaining necessary, sufficient, and suitable projects. The organization should define the security aspects of projects, accountabilities, and authorities. Then, it should identify new or modified security aspects of mission or business opportunities and prioritize or select opportunities based on security objectives and concerned. It should identify and allocate resources to achieve the security aspects of project goals and objectives. The security aspects of multi-project interfaces and dependencies that need management or support should be determined. The security aspects of project reporting requirements and review milestones that govern project execution should be communicated. Projects should be authorized to commence execution with consideration to the security aspects of the project plans. These security aspects should be regularly evaluated to confirm ongoing viability. Satisfactory projects should be continued while lackluster projects should be reconsidered or redirected. Projects whose security-driven disadvantages or risks outweigh the benefits brought to the organization, should be terminated. After completion of agreements for products or services, close the projects according to established security criteria, constraints, and considerations.

Human Resources Management (HR):

The *Human Resources Management* process provides the necessary human resources and ensures that their competence is consistent with business needs. System Security Engineering skills of current and prospective personnel should be identified based on the needs of current and expected projects. The organization should establish a plan to foster the development of System Security Engineering skills that includes training, education and mentoring resources. It should provide and document records of personnel skills. The organization should maintain and manage

skilled Systems Security Engineering personnel to staff ongoing projects. New personnel should be acquired as needed. Personnel should be assigned based on the needs of the project and the development needs of the staff.

Quality Management (QM):

The *Quality Management* process assures that products and services meet organizational and project quality objectives and that customers are satisfied. The organization should establish quality management objectives, security quality management policies, procedures, and standards, and security quality evaluation criteria and methods. It should define the responsibilities and authority for the implementation of security quality management and provide relevant resources and information. To assess the security quality management, the organizations should obtain and analyze assurance evaluation results according to the specified criteria. Customer security quality satisfaction should be monitored. It should periodically conduct reviews of project quality assurance activities to ensure compliance with standards, policies, and procedures. The status of security quality improvements to the products, processes, and services should also be monitored. If there is sufficient risk that security quality objectives will not be achieved, preventative measures can mitigate risk. If security quality management objectives are not met, corrective action must be taken. Preventative and corrective action should be monitored to completion and relevant stakeholders should be informed.

Knowledge Management (KM):

The *Knowledge Management* process is used to create the capabilities and assets that organizations need to capitalize on existing knowledge and exploit opportunities. Organizations should define the security aspects of the knowledge management strategy. It should identify security knowledge, skills and manageable knowledge assets as well as what projects benefit from the knowledge, skills, and knowledge assets. It should establish and maintain a classification for capturing and sharing knowledge and skills across the organization and it should use those capabilities. Similarly, a taxonomy should be applied to knowledge assets and they should be securely acquired and deployed to relevant areas of the organization. Security Knowledge, skills, and knowledge assets should be continuously monitored, recorded and reassessed according to the security aspects of technology and market needs.

Technical Management Processes:

Project Planning (PL):

The *Project Planning* process produces and coordinates effective and workable plans. The organization should begin by identifying the project security objective and constraints before defining the security aspects according to the scope as established in agreements and defining and maintaining a security view of the life cycle model and its constituent stages. The security activities and tasks of the work breakdown structure should be identified and all processes that will be applied to the project should be defined and maintained. The security aspects of the

project schedule, based on management and technical objectives, as well as work estimates, should be defined and maintained. The organization should also define the security achievement criteria and major dependencies on external input or output for life cycle stage decision gates, the security related costs of the project and how the budget is allocated to address those costs, the system engineering roles, responsibilities, accountabilities, and authorities, and the security aspects of the infrastructure and services required. The organization should outline the security aspects of the acquisition of materials and services from supplies external to the project. A plan for the project and technical management and execution, including reviews that address all security concerns, should be generated and communicated to the appropriate parties within the organization. Afterward, the organization should obtain authorization for the security aspects of the project and submit requests and obtain commitments for the resources required to perform the security aspects of the project. Finally, the project plan should be implemented and managed as directed.

Project Assessment and Control (PA):

The *Project Assessment and Control* process assesses whether plans are aligned and feasible, determines the status of a project or its performance, and directs the project execution to help ensure that the performance will satisfy technical objective plans while remaining within the projected budget. The organization begins by determining the security aspects of the project and control strategy and assessing the alignment of those aspects with the project objectives and plans with the project context. The security aspects to the management and technical plans should be assessed against the appropriate plans to determine the actual and projected cost, schedule, and performance variances. The adequacy of security roles, responsibilities, accountabilities and authorities within the project should also be assessed alongside the adequacy and availability of the resources allocated to the security aspects of the project. The organization should conduct the required management and technical reviews, audits, and inspections in full consideration of the project security aspects. The security aspects of critical processes and new technologies and the security aspects of process execution should be monitored. Security measurement results should be analyzed to inform recommendations. The results of security assessment tasks should be recorded and reported. The organization should take actions needed to address security concerns and replan the security aspects of the project if necessary. Based on the achievement of security objectives and performance measures, the organization should determine whether the project moves towards the next milestone or event.

Decision Management (DM):

The *Decision Management* process provides a structured, analytical framework for objectively identifying, characterizing, and evaluating a set of alternatives for decision making at any stage of the life cycle and for selecting the optimal solution. The organization should define the security aspects of the decision management strategy and identify the security aspects of the circumstance and need for a decision. The stakeholders with relevant security expertise should be

involved in the decision making. The security aspects of the decision management strategy should be compared to each decision in order to determine the desired security outcome and the measures of security selection criteria. The organization should determine the security aspects of the trade space and alternatives. Each alternative should be evaluated against the security criteria and the preferred alternative for each security-based decision should be selected. The organization should record the security-based assumptions, rationale, and resolutions. They should also record, track, and evaluate the security aspects of security-based decisions.

Risk Management (RM):

The *Risk Management* process is used to continuously identify, analyze, treat, and monitor risks. The organization begins the process by defining security aspects of the risk management strategy and by defining and recording the security context, security risk threshold and conditions, and risk profile. The stakeholders should be made aware of the risk profile based on their needs. The organization should identify security risks in the risk management categories and estimate the likelihood of occurrence and consequence for each risk. Each risk should then be evaluated against the security thresholds. The organization should define a risk treatment strategy and measures for each risk that does not meet its threshold. Options for risk treatments are recommended to and selected by informed stakeholders. The security risks accepted by stakeholders should be identified and monitored to determine whether future risk treatment is needed. The management of identified risk treatments should be coordinated across the organization. All risks, the risk management context, and emerging risks should be continuously monitored and evaluated for changes and effectiveness throughout the life cycle.

Configuration Management (CM):

The *Configuration Management* process is employed to manage and control system elements and configurations throughout the life cycle. The organization should define the security aspects relevant to the configuration management process, its approach for the secure archive and retrieval of configuration items, configuration management artifacts, data, and information, and the security aspects of baseline identifiers throughout the life cycle. It should identify the security aspects of system elements and information items that are configuration items, as well as identify the security aspects related to the hierarchy and structure of system information. The nomenclature for system, system element, and information item identifiers should be established. The organization should obtain acquirer and supplier agreements about security aspects to establish a baseline.

The organization should identify the security aspects of requests for change and requests for variance and it should determine how to respond to requests. The security aspects should be incorporated into requests before submission for approval. Requests and changes to baselines should be tracked and monitored. The organization should develop and maintain security-relevant configuration management status information for system elements, baselines, and

releases to be better able to capture, store, and report configuration management data. The need for security-focused configuration management audits should be established. The organization should verify that the system configurations satisfy security requirements. It should monitor the security aspects of incorporation of approved configuration changes. It should assess whether the system meets baseline security functionality and performance capabilities and whether the system conforms to the security aspects of operational and configuration information items. All audit results and disposition action should be recorded prior to the authorization for specific system use or the issue of system releases and deliveries. The security aspects of system releases should be tracked and monitored.

Information Management (IM):

The *Information Management* process is used to generate, obtain, confirm, transform, retain, retrieve, disseminate, and dispose of information to designated stakeholders. The organization should define its security aspects relevant to the information management strategy and define its protections for managed information items. The authorities and responsibilities of the security aspects of information management should be designated. The organization should also define its protections for specific information item content, format, and structure, and define the security aspects of its information maintenance actions. Next, the organization should securely obtain, develop, or transform the identified information items. It should securely maintain information items and their storage records, securely publish, distribute, or provide access to information items to designated stakeholders, securely archive designated information, and securely dispose of unwanted or invalid information or information that has not been validated.

Measurement (MS):

The *Measurement* process is used to collect, analyze, and report objective data and information for the express purpose of effective management and demonstrating the quality of products, services, and processes. The organization should define security aspects relevant to the measurement strategy, define procedures for data collection, analysis, access, and reporting of security-relevant data, and define the criteria for evaluating security-relevant information items and the processes used on them. It should describe the characteristics of the organization that are relevant to the security requirements and select and specify measures that satisfy the security-relevant information needs. It should identify and prioritize the security relevant needs. It should identify and plan for the need for enabling or supporting systems to facilitate measurement. Procedures for security-relevant data generation, collection, analysis and reporting should be integrated into relevant processes. The data should be collected, stored, verified, analyzed, and used to develop security-related information items. The security measurement results should be recorded and communicated to relevant users.

Quality Assurance (QA):

The *Quality Assurance* process helps ensure the effective application of an organization's *Quality Management* process. The organization should define relevant security aspects. This process should be independent from security quality assurance in other life cycle processes. Products and services should be evaluated for conformance to established criteria, contracts, standards, and regulations. The output of life cycle processes should be validated and verified to determine conformance with relevant security standards. The life cycle processes, tools, environment, and supplier process can then be evaluated for conformance to established criteria, contracts, standards, and regulations. In order to manage quality assurance, the organization should securely create, maintain, store, and distribute records and reports related to security aspects of quality assurance activities. The security aspects of incidents and problems associated with products, services, and product evaluations, should be identified, recorded, analyzed, classified, resolved, or elevated. Treatments of problems should be prioritized and tracked to closure. Stakeholders should be informed of the security status of incidents and problems.

Technical Processes:

Business or Mission Analysis Process (BA):

The *Business or Mission Analysis* process is used to define the business or mission opportunity or problem and to determine a viable solution. The phase begins with a review of the problems and opportunities presented to the organization with respect to the security objectives. Security aspects of the organization are used to define the problem, characterize potential solutions, and select the best solution. Next, the organization should identify, plan for, and gain access to enabling systems or services that will support the security aspects of the organization. The problem should be analyzed in the context of the security aspects and the measures of success to be achieved. Information from the concerns of stakeholders, from the mission, or from operations can be used to better understand the problem and the underlying security implications. Security aspects of potential solutions, and in stages of the life cycle of potential solutions, should be considered before deciding on a solution. Limitations, constraints, and alternative solutions should also be considered. Alternative solutions should be analyzed with regards to the security objectives and a preferred alternative solution should be selected in case the preferred solution fails. During the business and mission analysis, the organization should maintain bidirectional traceability of all security aspects and supporting data associated with business or mission problems or opportunities. Security relevant information should be used to baseline the decisions throughout the life cycle of the system.

Stakeholder Needs and Requirements Definition Process (SN):

The *Stakeholder Needs and Requirements Definition* process is used to define stakeholder requirements for a system that can provide the capabilities needed by users of that system in the target environment. The organization should identify stakeholders who have a security interest in

the system throughout its life cycle. A strategy should be developed to gather information from stakeholders and best meet their protection needs and security requirements. In order to define the stakeholder protection needs, the security concepts of use across all preliminary life cycle concepts should be defined. The definitions should inform the identification of all tangible and intangible stakeholder assets and asset classes. The assets should be prioritized according to the adverse consequences of asset loss. The asset susceptibility to adversity and uncertainty should be approximated throughout the life cycle and correlated with the concerns of the stakeholders. Stakeholder protection needs should then be identified in terms of the loss consequences realized by the stakeholders relative to the assets and the events that produce the loss consequences. Stakeholders should prioritize their protection needs and down-select the assets that warrant protection. The rationale informing the determination of protection needs and the prioritization of systems should be captured to document the reason behind each decision.

A representative set of scenarios should be developed to help identify the required protection capabilities and security measures that correspond to anticipated operational and other life cycle concepts. Next, the stakeholder protection needs should be transformed into security requirements by identifying security-oriented constraints on a system solution and then redefining the stakeholder needs in terms of the security concepts, life cycle concepts, scenarios, and constraints. The stakeholder security requirements should be analyzed in order to define critical security performance and assurance metrics that enable the assessment of technical achievement. Metadata can be applied to identify security requirements that contain security constraints. The stakeholders should provide consensus on whether all security requirements have been understood and satisfied. Any issues undermining consensus should be resolved. Explicit agreement on stakeholder security requirements should be obtained. Afterward, all asset protection data should be recorded to maintain traceability between stakeholder protection needs and security requirements. Finally, security-related information items should be used to baseline the systems.

System Requirements Definition Process (SR):

The *System Requirements Definition* process is used to transform the stakeholder and user-oriented views of desired capabilities into a view of a technical solution that meets the operational needs. The security aspects and functional boundaries of the system should be defined in terms of the security behavior and properties desired. The security domains and their correlation to the functional boundaries of the system should also be clarified in order to define a strategy based on the security requirements. Each security function that the system is required to perform should be specified along with the applicable security requirements, constraints, system requirements, and rationale. The system security requirements and associated constraints should be incorporated into the system requirements. Next, the system requirements should be analyzed according to the security concerns. Security-driven performance and assurance measures should be defined to enable assessment of technical achievement. Security-driven metadata can be used

to identify which system requirements are relevant to security. The analyzed requirements and the constraints should be presented to the stakeholders for review. Any issues with the requirements or constraints should be resolved. The stakeholders should provide an explicit agreement on the system security requirements and security-driven constraints. Traceability of these requirements and constraints should be maintained. Finally, security-relevant information items should be used to baseline the system.

Architecture Definition Process (AR):

The *Architecture Definition* process is used to generate one or more system architecture alternatives that encompass stakeholder concerns and system requirements. The process begins with the identification of the key drivers behind the security aspects of the system architecture and the identification of the stakeholder security concerns. Next, the security aspects of the architecture roadmap, approach and strategy are defined along with the evaluation criteria based on security concerns and security-relevant requirements. The organization should identify, plan for, and gain access to enabling systems or services to support the security aspects of the architecture.

The organization should define its philosophy of protecting the system at the architecture level. This may lead to an adaptation or alteration of the security viewpoints, based on the stakeholder security concerns. The security architecture framework used to model and develop the architecture should be identified and supporting security modeling tools and techniques should be selected or developed. The interfaces, interconnections, and interactions with external entities that collect into the security context and boundaries of the system should be defined. The relationship between entities should be identified and compared to stakeholder concerns and security requirements.

Security concepts, aspects, and constraints should be applied to architecture entities. Security models of candidate alternative architecture should be selected, adapted, or developed in accordance with stakeholder concerns, security requirements, and system requirements. The philosophy of architecture and the security model in which the architecture is developed should be aligned to prevent vulnerabilities. System security requirements should be allocated to the architecture and system elements. Security-relevant mapping can be used to capture security-driven characteristics and constraints that may be reflected in design patterns, reference designs, or models. The design principles for the system and the evolution of the system should reflect the philosophy of protection.

Each candidate architecture should be assessed against security requirements, constraints, and stakeholder concerns. Established security aspects should be used to baseline the system. The selected architecture should be governed by the security aspects and security related roles of accountability, authority, and responsibility. The security architecture should be completely maintained and its evolution should be organized, assessed, and controlled according to a

maintained definition of the security aspects and a defined evaluation strategy. Traceability of the security aspects of the architecture should be maintained and the information items should be retained to baseline the system.

Design Definition Process (DE):

The *Design Definition* process is used to provide detailed data about a system and its elements to enable the implementation consistent with architectural entities according to the models and views of the system architecture. The philosophy of protection should be determined and applied at the design level. The organization should determine the security technologies required for each element of the system. Next, the principles of secure system evolution and of the design definition strategy should be clearly defined. Enabling systems or services needed to support the security aspects of the definition process should be identified, acquired, or accessed. System security requirements should be applied to system elements to transform the system architecture characteristics into security design characteristics. Necessary security design enablers should be defined and security design alternatives should be examined. Any security interfaces between system elements and external entities should be defined or redefined. The interfaces reflect the level of detail needed to make architecture decisions and they help to develop security design artifacts, such as documents and databases.

The organization can begin assessing the alternatives to obtaining security relevant system elements by identifying relevant security-relevant non-developmental items (NDI) and assessing them against the security requirements and criteria. The preferred alternative among candidate NDI solutions and design alternatives for system elements should be determined. Then security design characteristics should be mapped to system elements. The security design and rationale behind decisions should be documented. Traceability of the security aspects of the definition should be maintained and the information items should be retained to baseline the system.

System Analysis Process (SA):

The *System Analysis* process provides a rigorous basis for data and information for technical understanding and decision making throughout the system life cycle. The stakeholders, security aspects, and problem should be identified and then the objective, scope, level of fidelity, and level of security assurance should be determined. Security aspects of the system analysis should be defined and used to select a method of analysis. Enabling or supporting systems should be acquired or accessed and the data needed for system analysis should be collected.

The security aspects of system analysis are performed by identifying and validating security assumptions, by applying the selected analysis methods, by reviewing the security aspects of the system analysis for quality and validity, and by developing conclusions, recommendations and rationale based on the results. Traceability of the security aspects of the

analysis should be maintained and the information items should be retained to baseline the system.

Implementation Process (IP):

The *Implementation* process helps to realize a specific system element. The organization should develop security aspects pertinent to the implementation strategy, identify constraints on the system requirements, design, or architecture based on those security aspects, and identify, acquire, or access supporting or enabling systems to address those constraints. Hardware, software, and firmware system elements should be realized or adapted in accordance with the security aspects, implementation procedures, and constraints. System elements should be securely packaged or stored to preserve their security characteristics until they are needed. Evidence should be recorded to substantiate claims that the system requirements are in accordance with system architecture, security design, and all associated security concerns. Security aspects of implementation results and anomalies should also be recorded. Traceability of the security aspects of the implementation activities should be maintained and the information items should be retained to baseline the system.

Integration Process (IN):

The *Integration* stage is used to synthesize a set of elements into a realized system in a manner that satisfies system requirements, architecture, and design. Organizations begin by identifying and defining the checkpoints for the trustworthy and secure operation of the assembled interfaces and selected systems. Next, the security aspects of the integration strategy are developed. Enabling and supporting systems are identified, acquired, or accessed, to support the integration strategy. The constraints resulting from the security aspects of integration are incorporated into the security requirements, architecture, or design. System elements are obtained in accordance with the security criteria and requirements established in agreements and schedules. The implemented systems are assembled in secure configurations and their characteristics, interfaces, functional behavior, and behavior across interfaces is checked according to the security characteristics. The security results of the integration, including any anomalies, are recorded. The traceability of security aspects of integrated system elements is maintained to provide evidence that supports assurance and trustworthiness claims. Security related information items are used to baseline systems.

Verification Process (VE):

The *Verification* process provides objective evidence that a system or system element fulfills its specific characteristic or requirement. The organization identifies security aspects, the verification scope, security-focused verification actions, and the constraints that could limit the feasibility of verification actions. The most appropriate methods or techniques are selected from amongst the security focused verification actions according to the security criteria. The security aspects of the verification strategy are defined. The system constraints resulting from the security

aspects are defined and used to identify, acquire, or access enabling or supporting systems or services that support the security aspects of verification.

The security aspects of verification procedures are defined, each supporting one or more security-focused verification actions. The security verification procedures are performed and the results, including any anomalies, are recorded. The security characteristics of operational incidents and problems are also recorded and are tracked to resolution. Stakeholders then provide an agreement that the system meets the specified security criteria and requirements. The traceability of security aspects of verified system elements is maintained to provide evidence that supports assurance and trustworthiness claims. Security related information items are used to baseline systems.

Transition Process (TR):

The *Transition* process establishes a capability for a system to provide services specified by the stakeholder requirements in the operational environment. The security aspects of the transition strategy are developed and used in the identification of facility or site changes, of constraints on the incorporation of security aspect of the transition into the system, architecture, or design, and of the training necessary to secure, sustain, support, and utilize systems or system elements. Enabling or supporting systems should be identified, acquired, or accessed. The facility should be prepared according to security installation requirements and then the system should be securely delivered and installed at the specified location with demonstrative security requirements. Stakeholders should be provided security training on how to interact with the system and shown that the system is capable of delivering the desired protection capability and that it is sustainable according to the enabling systems. The security aspects of the system operational readiness should be reviewed and if approved, the system should be commissioned for operation. The security aspects of the transition results, anomalies, operational incidents, and problems should be recorded and tracked. The traceability of security aspects of transition system elements is maintained to provide evidence that supports assurance and trustworthiness claims. Security related information items are used to baseline systems.

Validation Process (VA):

The *Validation* process provides objective evidence that the system fulfills the business or mission objectives when in use and that stakeholder requirements concerning the intended use and operation in the environment, are achieved. The organization can prepare by identifying the security aspects of validation, identifying the scope and the corresponding security-focused validation actions, identifying the constraints that limit the feasibility of those actions, and by selecting the appropriate methods or techniques for the security aspects of validation and the associated security criteria for each security-focused validation action. Additionally, system constraints resulting from the security aspects of validation should be incorporated into the stakeholder security requirements and used to select enabling or supporting systems to acquire

the security aspects of validation. The security aspects of validation procedures should be defined and then the procedures should be performed in the defined environment. The results, anomalies, operational incidents, and problems should be recorded and tracked. The traceability of security aspects of validated system elements should be maintained to provide evidence that supports assurance and trustworthiness claims. Security related information items are used to baseline systems.

Operation Process (OP):

The *Operation* process is used to utilize the system to deliver its services. The organization can prepare for secure operation by defining the security aspects of the operational strategy, by identifying constraints resulting from those security aspects and incorporating them into the system requirements, architecture, and design, and by identifying and defining the security training and qualification requirements for system operation. Afterward, the system should be securely used in the intended operational environment. Materials and other resources should be applied, as required, to operate the system securely and sustainably. The organization should monitor the security aspects of system operation, and identify and record when system security performance is not within acceptable security parameters. If necessary security contingency operations should be performed. The results of secure operation, any anomalies, operational incidents, or problems should be recorded and tracked. The traceability of security aspects of operational system elements should be maintained to provide evidence that supports assurance and trustworthiness claims. Security related information items are used to baseline systems. Additionally, the organization should provide security assistance and consultation to customers upon request. The results and subsequent results of the support should be recorded and used to determine the degree to which the delivered systems or security services satisfy the needs of the customer.

Maintenance Process (MA):

The *Maintenance* process is used to sustain the capability of the system and to provide a service. The organization should define the security aspects of the maintenance strategy and identify the system constraints resulting from the security aspects of maintenance and logistics and incorporate the constraints into the system requirements, architecture, and design. Trades in security aspects of maintenance and logistics that result in a solution that is trustworthy, secure, affordable, operable, supportable, and sustainable, should be explored. Enabling or supporting systems or services should be identified. Incident and problem reports should be reviewed and used to identify the security relevance and associated maintenance needs. The security aspects of incidents and problems should be recorded and tracked to resolution. Procedures to correct random faults or to regularly replace system elements to ensure the ability to deliver system security functions or services, should be implemented, along with actions to restore the system to secure operational status when a random fault causes a system failure. The organization should perform preventative maintenance by replacing or servicing system elements prior to failure with

security related impact. It should also perform failure identification actions when security noncompliance has occurred within the system.

The organization should perform the security aspects of acquisition logistics and operational logistics. It should implement any secure packaging, handling, storage, and transportation needed during the life cycle of the system. It should confirm that security aspects incorporated into logistics actions satisfy the required protection levels such that system elements are securely stored and are able to meet repair rated and planned schedules. Additionally, it should confirm that the security aspects of logistics actions include security supportability requirements that are planned, resourced, and implemented. The security aspects of maintenance and logistics should be recorded along with any anomalies, operational incidents, or problems. The information should be used to identify and record security-related trends in incidents, problems, and maintenance and logistic actions. The traceability of security aspects of maintenance system elements should be maintained to provide evidence that supports assurance and trustworthiness claims. Security related information items are used to baseline systems. Finally, customer satisfaction should be monitored according to the security aspects of system performance and maintenance support.

Disposal Process (DS):

The *Disposal* process is used to end the existence of a system element or system for a specified intended use, to appropriately handle replaced or retired elements, or to meet identified critical disposal needs according to an agreement, organizational policy, or for environmental, legal, safety, or security concerns. The organization should develop the security aspects of the disposal strategy according to its needs. Constraints resulting from the security aspects should be identified and incorporated into the system requirements, architecture, and design. Enabling or supporting systems or services that support the secure disposal strategy should be identified, acquired, or accessed. The organization should specify secure storage criteria for any system that needs to be stored. Measures should be taken to preclude terminated personnel or disposed system elements from being returned to service. To dispose of a system or system element, the organization should begin by deactivating the element and removing it from the surrounding systems or elements. Impacted operating staff should be securely withdrawn from the system and their relevant operational knowledge of the system should be recorded. System elements and life cycle artifacts, appropriate to the disposal action, should be sanitized. System elements and their parts that are not intended for reuse should be prevented from reentering the supply chain. The organization should confirm that no unresolved security factors exist following the disposal of a system before returning the environment to its initial state or an elevated security state. Information generated throughout the life cycle of the system should be archived and protected.

Conclusion:

It is the responsibility of every senior executive to encourage a vigilant and security centric organizational culture. It is the responsibility of each individual to use cyber hygienic practices that thwart threat and it is absolutely necessary for security professionals to conjure the moral courage needed to speak up when optimal security mechanisms are not implemented and vulnerabilities lay wide open for adversarial exploitation. With the technologies and layering techniques so readily available, there are no longer any justifications for organizations that possess gaping vulnerabilities throughout their network. It is imperative that security professionals take time to study and apply these and other standards and strategies that will accelerate the velocity in which companies catch up with and combat bad actors in this continuously compounding threat landscape.

Contact Information

Legislative Branch Inquiries:

- James Scott, Senior Fellow, ICIT (james@icitech.org, 202-774-0848)

Federal Agencies, Executive Branch and Fellow Inquiries:

- Parham Eftekhari, Senior Fellow, ICIT (parham@icitech.org, 773-517-8534)

Links

Website: www.icitech.org



<https://twitter.com/ICITorg>



<https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit->



<https://www.facebook.com/ICITorg>