Overview of NIST SP 800-160, Volume 1

Victoria Yan Pillitteri
victoria.yan@nist.gov
November 20, 2019
Overview of NIST SP 800-160, Volume 1


- **Background**
- System Security Engineering **Fundamentals**
- **System Life Cycle Processes**
- **Related** NIST publications
- **Contact** Information and **Questions**
BACKGROUND

Systems Security Engineering (1 of 2)

- A **specialty engineering** discipline of systems engineering
- **System security** is the application of engineering and management principles, concepts, criteria, and techniques to optimize security within constraints of operational effectiveness, time, and cost throughout all stages of the system life cycle.
- **Systems security engineering** focuses on the protection of stakeholder and system assets in order to exercise control over asset loss and the associated consequences.
- Provides a **fully integrated, system-level perspective** of system security.
Systems Security Engineering (2 of 2)

As part of a multidisciplinary systems engineering effort:

- Defines stakeholder security objectives, protection needs/concerns, security requirements, and validation methods;
- Defines system security requirements and verification methods;
- Develops security views /viewpoints of the system architecture/design;
- Identifies/assesses vulnerabilities to life cycle disruptions, hazards, and threats;
- Designs proactive and reactive security functions to control asset loss and associated loss consequences;
- Provides security considerations to inform systems engineering efforts;
- Identifies/quantifies/evaluates the costs/benefits of security functions to inform analysis of alternatives, engineering trade-offs, and risk treatment decisions;
- Performs system security analyses in support of decision making;
- Demonstrates through evidence-based reasoning, that security claims for the system have been satisfied;
- Provides evidence to substantiate claims for the trustworthiness of the system; and
- Leverages multiple security and other specialties to address all feasible solutions in order to deliver a trustworthy, secure system.
Objective of NIST SP 800-160, Volume 1

- Formalize systems security engineering principles, concepts and activities
- Provide considerations and demonstrate how systems security engineering can be applied to systems engineering activities;
System-related constructs

- **system**
  - Combination of interacting elements organized to achieve one or more stated purposes

- **system element**
  - Member of a set of elements that constitute a system

- **system-of-interest**
  - System that is the focus of the systems engineering effort

- **enabling system**
  - System that supports a system-of-interest during its life cycle stages but does not necessarily contribute directly to its function during operation

- **other system**
  - System that interacts with the system-of-interest in its operational environment

System Engineering view of the system-of-interest
System Life Cycle Processes and Life Cycle Stages

System Life Cycle Processes

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquisition</td>
<td>Life Cycle Model Management</td>
<td>Project Planning</td>
<td>Business or Mission Analysis</td>
</tr>
<tr>
<td>Supply</td>
<td>Infrastructure Management</td>
<td>Project Assessment and Control</td>
<td>Stakeholder Needs and Requirements Definition</td>
</tr>
<tr>
<td></td>
<td>Portfolio Management</td>
<td>Decision Management</td>
<td>System Requirements Definition</td>
</tr>
<tr>
<td></td>
<td>Human Resource Management</td>
<td>Risk Management</td>
<td>Architecture Definition</td>
</tr>
<tr>
<td></td>
<td>Quality Management</td>
<td>Configuration Management</td>
<td>Design Definition</td>
</tr>
<tr>
<td></td>
<td>Knowledge Management</td>
<td>Information Management</td>
<td>System Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Measurement</td>
<td>Implementation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Quality Assurance</td>
<td>Integration</td>
</tr>
</tbody>
</table>

Life Cycle Stages

- Concept
- Development
- Production
- Utilization
- Support
- Retirement

System life cycle processes

*Recursive, iterative, concurrent, parallel, sequenced execution*

<table>
<thead>
<tr>
<th>Agreement Processes</th>
<th>Organizational Project-Enabling Processes</th>
<th>Technical Management Processes</th>
<th>Technical Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquisition</td>
<td>Life Cycle Model Management (Mgmt)</td>
<td>Project Planning</td>
<td>Business or Mission Analysis</td>
</tr>
<tr>
<td>Supply</td>
<td>Infrastructure Mgmt</td>
<td>Project Assessment &amp; Control</td>
<td>Stakeholder Needs &amp; Requirements (Reqs) Definition</td>
</tr>
<tr>
<td></td>
<td>Portfolio Mgmt</td>
<td>Decision Mgmt</td>
<td>System Reqs Definition</td>
</tr>
<tr>
<td></td>
<td>Human Resource Mgmt</td>
<td>Risk Mgmt</td>
<td>Architecture Definition</td>
</tr>
<tr>
<td></td>
<td>Quality Mgmt</td>
<td>Configuration Mgmt</td>
<td>System Analysis</td>
</tr>
<tr>
<td></td>
<td>Knowledge Mgmt</td>
<td>Information Mgmt</td>
<td>Implementation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Measurement</td>
<td>Integration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Quality Assurance</td>
<td>Verification</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Transition</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Validation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Operation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Disposal</td>
</tr>
</tbody>
</table>

3.1.1 Acquisition Process

Purpose

“The purpose of the Acquisition process is to obtain a product or service in accordance with the acquirer's requirements.”


Systems Security Engineering Purpose

Systems security engineering, as part of the Acquisition process, ensures protection needs and security concerns are addressed by the acquirer’s request to obtain a product or service.

Systems Security Engineering Outcome

- Security considerations are addressed by the acquisition strategy.

- A request for a supplier to provide a product or service includes security.

Systems Security Engineering Activities and Tasks

AQ-1 PREPARE FOR SECURITY ASPECTS OF THE ACQUISITION

AQ-1.1 Define the security aspects for how the acquisition will be conducted.

Discussion: The security aspects include how security objectives, protection needs, and security...
**SYSTEM LIFE CYCLE PROCESSES**

**Systems Security Engineering Activities and Tasks**

**AQ-1** PREPARE FOR SECURITY ASPECTS OF THE ACQUISITION

**AQ-1.1** Define the security aspects for how the acquisition will be conducted.

**Discussion:** The security aspects include how security objectives, protection needs, and security concerns are achieved by the acquisition strategy. Security concerns and considerations impact and are impacted by the objectives and scope of the engineering effort; the *life cycle models* to be used; the acquisition activities, milestones, gates, and associated review and approval criteria; the protection of data, information, and information assets; risk and issues mitigation; the selection of suppliers; and acceptance conditions. Real-life demonstrations of compliance or conformance to laws, directives, regulations, policies, or other criteria. The acquisition strategy may describe life cycle models; liabilities; requirements or processes; levels of criticality; levels of trustworthiness and assurance; and prioritized relevant trade factors.

**References:** ISO/IEC/IEEE 15288, Section 6.1.1.3 a); ISO/IEC 15026; ISO/IEC 27036.

**Related Publications:** ISO/IEC 12207, Section 6.1.1.3.1; ISO/IEC 21827.
Draft NIST Special Publication 800-160, Volume 2

Developing Cyber Resilient Systems: A Systems Security Engineering Approach

Supplement NIST SP 800-160, Vol 1 & NIST SP 800-37

Identify cyber resiliency considerations
to support the engineering of trustworthy systems that depend on cyber resources

Includes cyber resiliency fundamentals, guidance in practice, use cases, and mappings
provides background, deep dive into constructs (goals, objectives, techniques & approaches, and design principles), and mappings to SP 800-53 security controls and threat frameworks.
NIST Special Publication 800-39
*Managing Information Security Risk – Organization, Mission, and Information System View*

- Multi-tiered risk management approach
- Identifies risk management process: frame, assess, respond and monitor
- Implemented by the Risk Executive Function
- Enterprise Architecture and SDLC Focus
- Supports all steps in the RMF (NIST SP 800-37)
NIST Special Publication 800-37, Rev. 2

- A holistic and comprehensive risk management process
  - Can be used to communicate across an organization (C-Suite to the systems/operations)
  - Aligns the Cybersecurity Framework to the RMF
  - Includes privacy, supply chain and security engineering

- Integrates the Risk Management Framework (RMF) into the system development lifecycle

- Provides processes (tasks) for each of the steps (Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor)
NIST Special Publication 800-53, Rev. 4
Security and Privacy Controls for Information Systems and Organizations

• **Catalog** of security and privacy controls
  - Not focused on any specific technologies or implementations
  - Can be applied to any kind of system

• Defines **three security baselines** (Low, Moderate, High)
  - Baseline for use determined by:
    ◦ information and system categorization (impact)
    ◦ organizational risk assessment and risk tolerance
    ◦ system-level risk assessment

• Some controls from the catalog are not included in any baseline

---

*NIST SP 800-53, Rev. 5 Final Draft is currently in review – there are changes for improved usability, address emerging threats, emphasize privacy and supply chain risk management, and systems security engineering.*
# NIST Special Publication 800-53, Rev. 4

*Security and Privacy Controls for Information Systems and Organizations*

## SP 800-53, Rev. 4 Control Families

<table>
<thead>
<tr>
<th>Control Family</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC – Access Control</td>
<td>PL – Planning</td>
</tr>
<tr>
<td>AT – Awareness and Training</td>
<td>PM – Program Management</td>
</tr>
<tr>
<td>AU – Audit and Accountability</td>
<td>PS – Personnel Security</td>
</tr>
<tr>
<td>CA – Security Assessment and Authorization</td>
<td>RA – Risk Assessment</td>
</tr>
<tr>
<td>CM – Configuration Management</td>
<td>SA – System and Service Acquisition</td>
</tr>
<tr>
<td>CP – Contingency Planning</td>
<td>SC – System and Communication Protection</td>
</tr>
<tr>
<td>IA – Identification and Authentication</td>
<td>SI – System and Information Integrity</td>
</tr>
<tr>
<td>IR – Incident Response</td>
<td>AP* – Authority and Purpose</td>
</tr>
<tr>
<td>MA – Maintenance</td>
<td>AR* – Accountability, Audit, and Risk Management</td>
</tr>
<tr>
<td>MP – Media Protection</td>
<td>DI* – Data Quality and Integrity</td>
</tr>
<tr>
<td>PE – Physical and Environmental Protection</td>
<td>DM* – Data Minimization and Retention</td>
</tr>
</tbody>
</table>
NIST Cybersecurity Framework (CSF)

The CSF is **voluntary** guidance, **based on existing standards, guidelines, and practices** for organizations to better manage and reduce cybersecurity risk.

[Related Publications](https://www.nist.gov/cyberframework)

cyberframework@nist.gov
NIST Mission

To promote **U.S. innovation** and **industrial competitiveness** by advancing **measurement science, standards, and technology** in ways that enhance economic security and improve our quality of life.
NIST Laboratory Programs

- Material Measurement Laboratory
- Physical Measurement Laboratory
- Engineering Laboratory
- Information Technology Laboratory
- Communication Technology Laboratory
- Center for Nanoscale Science and Technology
- NIST Center for Neutron Research

**Metrology Laboratories**
Driving Innovation through measurement science

**Technology Laboratories**
Accelerating the adoption and deployment of advanced technology solutions

**National User Facilities**
Providing world class, unique, user facilities
NIST ITL Computer Security and Applied Cybersecurity Divisions

Computer Security Division Mission: To provide standards and guidelines, tools, metrics, and practices to protect information and information systems.

Applied Cybersecurity Division Mission: Implements practical cybersecurity and privacy through outreach & the effective application of standards and best practices necessary for the U.S. to adopt cybersecurity capabilities.
# Cybersecurity Standards and Guidance

## Participation in Cybersecurity Standards Development Organizations (SDOs)*

- ANSI
- ISO
- IEC
- IEEE
- IETF
- TCG
- W3C
- 3GPP

*voluntary consensus SDOs; not all SDOs listed

## NIST-published Cybersecurity Guidance

- Federal Information Processing Standards (FIPS)
- Special Publications (SP)
- Interagency Reports (IR)
NIST-published Cybersecurity Guidance

**Federal Information Processing Standards (FIPS)**
- Developed when required by statute and/or there are compelling federal government requirements for cybersecurity

**Special Publications (SP)**
- Guidelines, technical specifications, recommendations and reference materials
- Multiple sub-series:
  - **SP 800**: developed to address and support the security and privacy needs of U.S. Federal Government information and systems.
  - **SP 1800**: “how to” guides that demonstrate how to implement and apply standards-based cybersecurity technologies
  - **SP 500**: information technology

**Interagency Reports (IR)**
- Reports of research findings, including background information for FIPS and SPs.