MISSION DRIVEN SECURITY: BASELINE ASSURANCE AND THREAT/VULNERABILITY

20190813 (BREFLET 029)

David Olmstead, PE, CPP, CISSP-ISSEP, ESEP, C|EH
Systems Engineer, Senior Staff

LOCKHEED MARTIN

SYSTEM SECURITY SYSTEMS ENGINEERING

MFC CYBER SECURITY

SYSTEMS ENGINEERING

PERMIT ME TO INTRODUCE MYSELF,

SYSTEM SECURITY SYSTEMS ENGINEERING

David Olmstead
Systems Engineer, Senior Staff
Systems Security Specialty Engineering

Lockheed Martin Missiles and Fire Control
5600 Sand Lake Road, MP-914, Orlando, FL 32819-1380
Email: david.olmstead@lmco.com
Phone: 407-356-4526

COMMONWEALTH OF PENNSYLVANIA
REGISTERED PROFESSIONAL
DAVID OLMSTEAD
ENGINEER
PE035294E

CPP® Certified Protection Professional
BOARD CERTIFIED IN SECURITY MANAGEMENT

CISSP® Certified Information Systems Security Professional
ISSEP® Engineering

C|EH™ Certified Ethical Hacker

EXPERT INCOSE ESEP SYSTEMS ENGINEERING PROFESSIONAL™

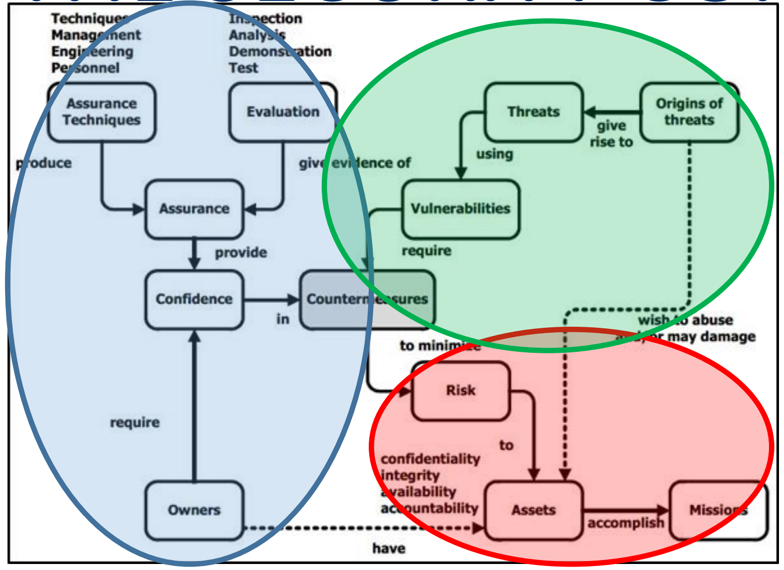
22nd ANNUAL
SYSTEMS & MISSION ENGINEERING CONFERENCE

- **Mission Driven Security: Baseline Assurance and Threat/Vulnerability Abstract**

- **A call for the application of both Mission Driven Security types: Baseline Assurance and Threat/Vulnerability methods.**
  - **We shall explore the hidden "Open Source" model of the "security context of the system" in IEEE Standard for System, Software, and Hardware Verification, and Validation (IEEE Std 1012-2016) and its application to Cybersecurity as a more complete solution.**
  - **Within the model we see the application of both Mission Driven Security types:**
    - Baseline Assurance methods and Threat/Vulnerability methods.
    - The model also is supported by the process defined by CNSSI 1253 Chapter 3 (as long as we apply the process including the need to Tailor).

Recognize the Correct Answer When Told

IEEE STD 1012™-2016, (INFORMATIVE) FIGURE J.1 THE SECURITY CONTEXT OF THE SYSTEM



There are two (2) entrances to "Countermeasures"

- "Baseline" Assurance to give Owners Confidence in the System-of-Interest
- Threats that use Vulnerabilities and Require Countermeasures

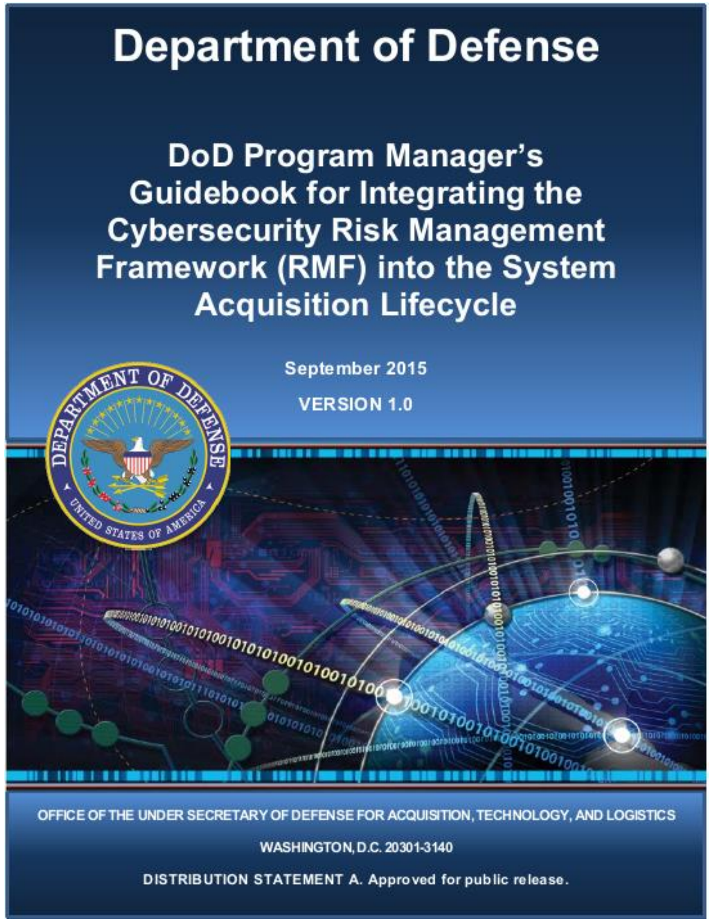
Both are "Mission Driven"

- One of the objectives of security analysis performed by the V&V effort is to verify that the system-required threat controls and safeguards are correctly implemented and to validate that they provide the desired levels of protection of system vulnerabilities. The other objective is to verify that there is a process for describing the system, software, and hardware process security.
- A system should consider different security issues in each phase of the life cycle because the system owner may change as the product evolves. The V&V security analysis should consider:
  - The context of the system (e.g., the development process and environment, the final operational environment, organization structures and management policy, operational and maintenance personnel roles, interfaces with other external systems or support systems);
  - The system of interest and its elements, threats, vulnerabilities, and countermeasures;
  - Tradeoffs between techniques, operations, and management to address security requirements.
  - Identification of threats. These threats may be natural (e.g., inclement weather, earthquakes), human (e.g., unintended or malicious), or environmental (e.g., chemical leak, power loss).

Cybersecurity (i.e., Security Context) is "Built Into" Verification and Validation

DoD PROGRAM MANAGER'S GUIDEBOOK FOR INTEGRATING THE CYBERSECURITY RISK MANAGEMENT FRAMEWORK (RMF) INTO THE SYSTEM ACQUISITION LIFECYCLE, 20150900

- Executive Summary
  - "This guidebook emphasizes integrating cybersecurity activities into existing processes including requirements, SSE, program protection planning, trusted systems and networks analysis, developmental and operational test and evaluation, financial management and cost estimating, and sustainment and disposal."
- Guidebook Key Tenets
  - "Cybersecurity requirements are treated like other system requirements"
  - "As the system matures and security controls are selected, implemented, assessed, and monitored, the PM collaborates with the authorizing official (AO) … to ensure the continued alignment of cybersecurity in the technical baselines, system security architecture, data flows, and design"
- "Failure to do [cybersecurity] early in the system lifecycle impacts the AO's authorization decision as well as system performance, and program cost and schedule."



Department of Defense

DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle

September 2015

VERSION 1.0

OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS

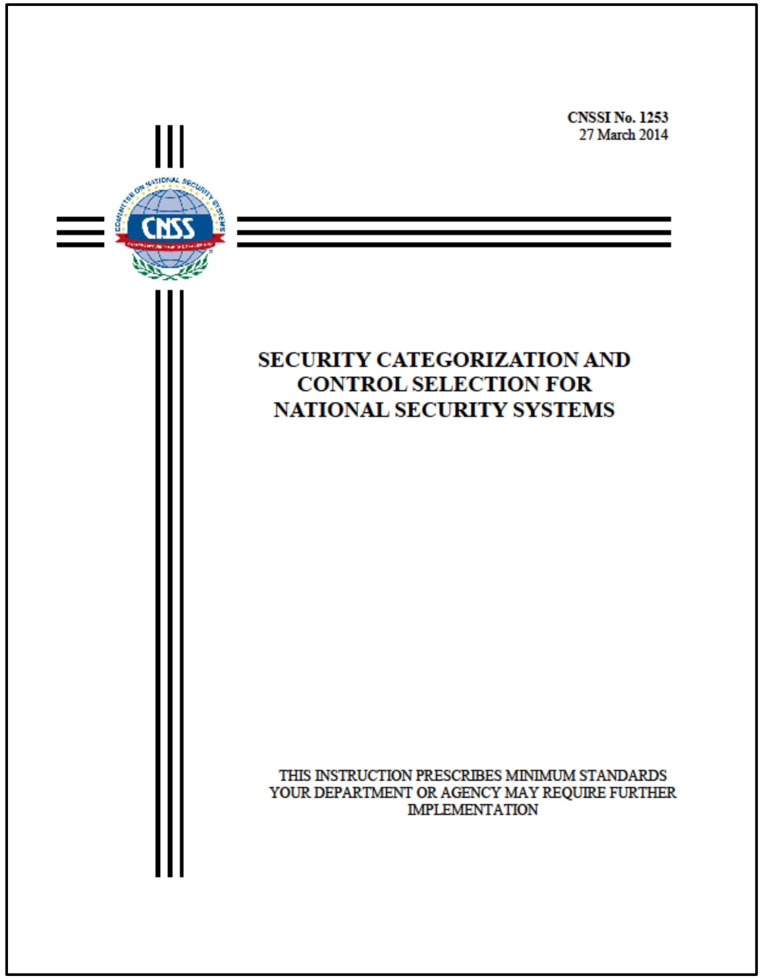
WASHINGTON, D.C. 20301-3140

DISTRIBUTION STATEMENT A. Approved for public release.

Eschew Suboptimization; Do Cybersecurity Early for an Optimum Total System Solution

CYBERSECURITY SOURCE DOCUMENTS

CNSSI 1253, 20140327

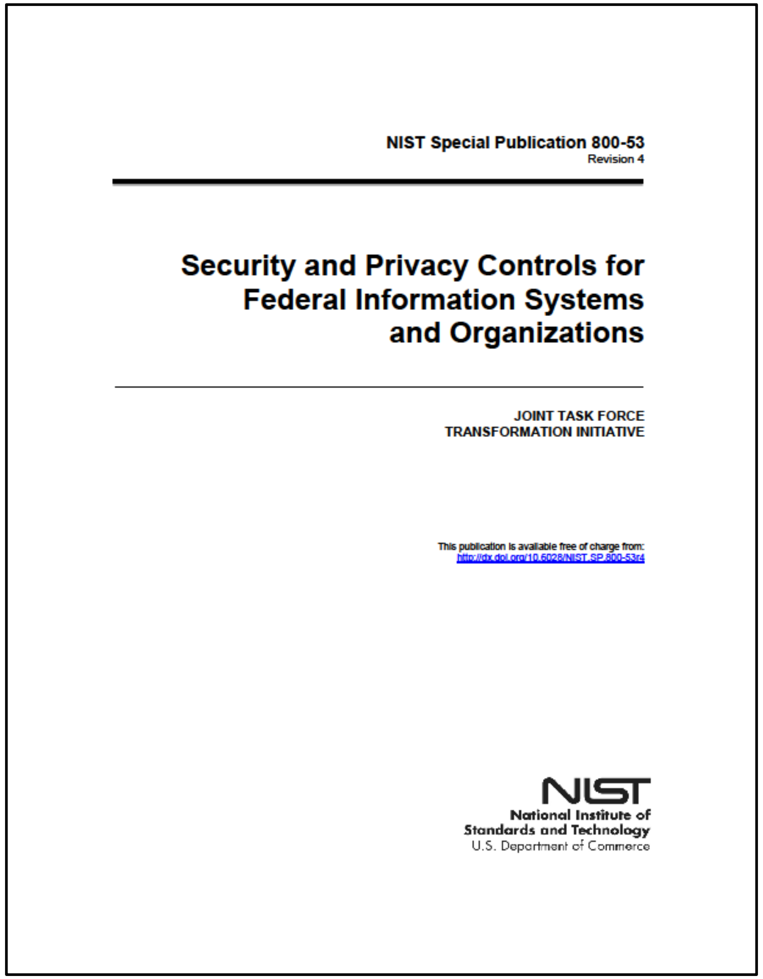


CNSSI No. 1253
27 March 2014

SECURITY CATEGORIZATION AND
CONTROL SELECTION FOR
NATIONAL SECURITY SYSTEMS

THIS INSTRUCTION PRESCRIBES MINIMUM STANDARDS
YOUR DEPARTMENT OR AGENCY MAY REQUIRE FURTHER
IMPLEMENTATION

NIST SP 800-53r4



NIST Special Publication 800-53
Revision 4

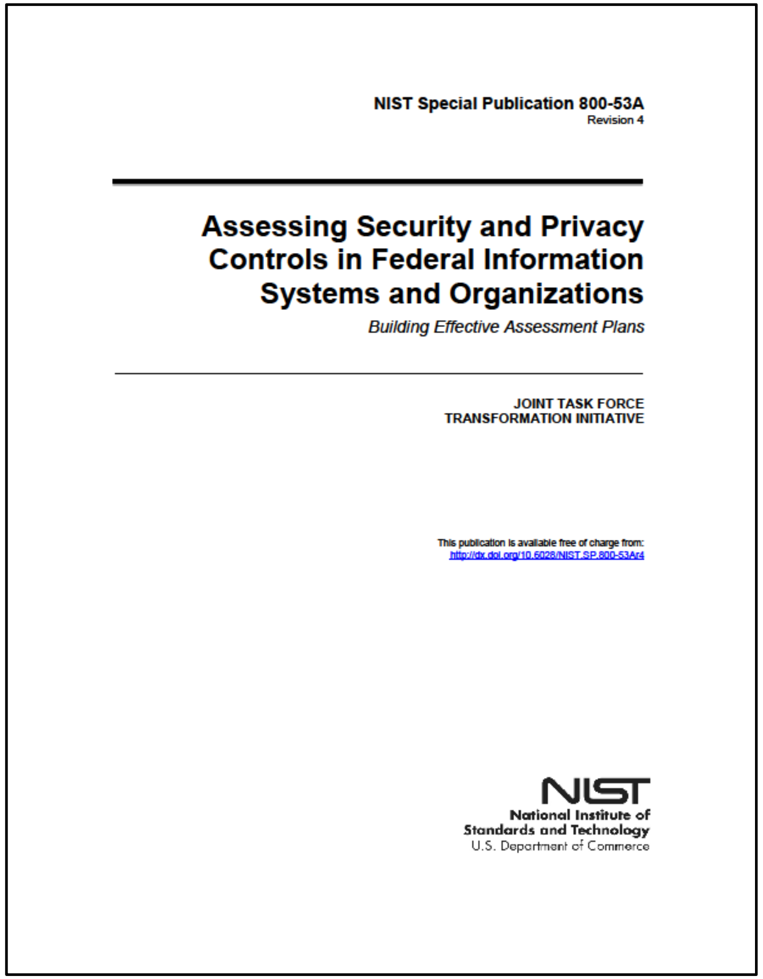
Security and Privacy Controls for
Federal Information Systems
and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

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

NIST SP 800-53Ar4



NIST Special Publication 800-53A
Revision 4

Assessing Security and Privacy
Controls in Federal Information
Systems and Organizations

Building Effective Assessment Plans

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

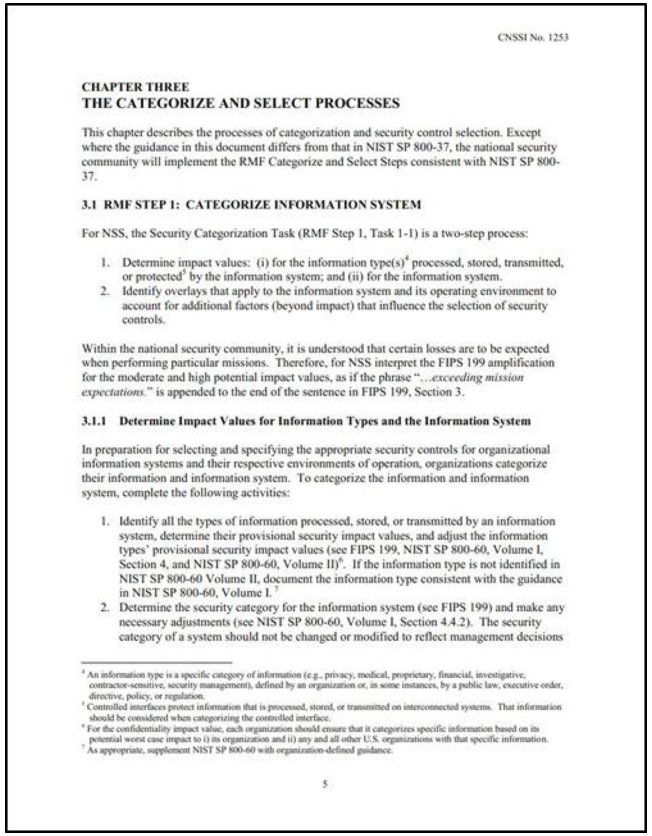
This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53Ar4

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

“Baseline” Assurance to give Owners “Confidence” in the System-of-Interest

CNSSI 1253, 20140327
CHAPTER 3, THE CATEGORIZE AND SELECT PROCESSES

Page 5



CNSSI No. 1253

CHAPTER THREE
THE CATEGORIZE AND SELECT PROCESSES

This chapter describes the processes of categorization and security control selection. Except where the guidance in this document differs from that in NIST SP 800-37, the national security community will implement the RMF Categorize and Select Steps consistent with NIST SP 800-37.

3.1 RMF STEP 1: CATEGORIZE INFORMATION SYSTEM

For NSS, the Security Categorization Task (RMF Step 1, Task 1-1) is a two-step process:

1. Determine impact values: (i) for the information type(s)[4] processed, stored, transmitted, or protected[5] by the information system; and (ii) for the information system.
2. Identify overlays that apply to the information system and its operating environment to account for additional factors (beyond impact) that influence the selection of security controls.

Within the national security community, it is understood that certain losses are to be expected when performing particular missions. Therefore, for NSS interpret the FIPS 199 amplification for the moderate and high potential impact values, as if the phrase "*…exceeding mission expectations.*" is appended to the end of the sentence in FIPS 199, Section 3.

3.1.1 Determine Impact Values for Information Types and the Information System

In preparation for selecting and specifying the appropriate security controls for organizational information systems and their respective environments of operation, organizations categorize their information and information system. To categorize the information and information system, complete the following activities:

1. Identify all the types of information processed, stored, or transmitted by an information system, determine their provisional security impact values, and adjust the information types' provisional security impact values (see FIPS 199, NIST SP 800-60, Volume I, Section 4, and NIST SP 800-60, Volume II)[6]. If the information type is not identified in NIST SP 800-60 Volume II, document the information type consistent with the guidance in NIST SP 800-60, Volume I.[7]
2. Determine the security category for the information system (see FIPS 199) and make any necessary adjustments (see NIST SP 800-60, Volume I, Section 4.4.2). The security category of a system should not be changed or modified to reflect management decisions

[4] An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor-sensitive, security management), defined by an organization or, in some instances, by a public law, executive order, directive, policy, or regulation.

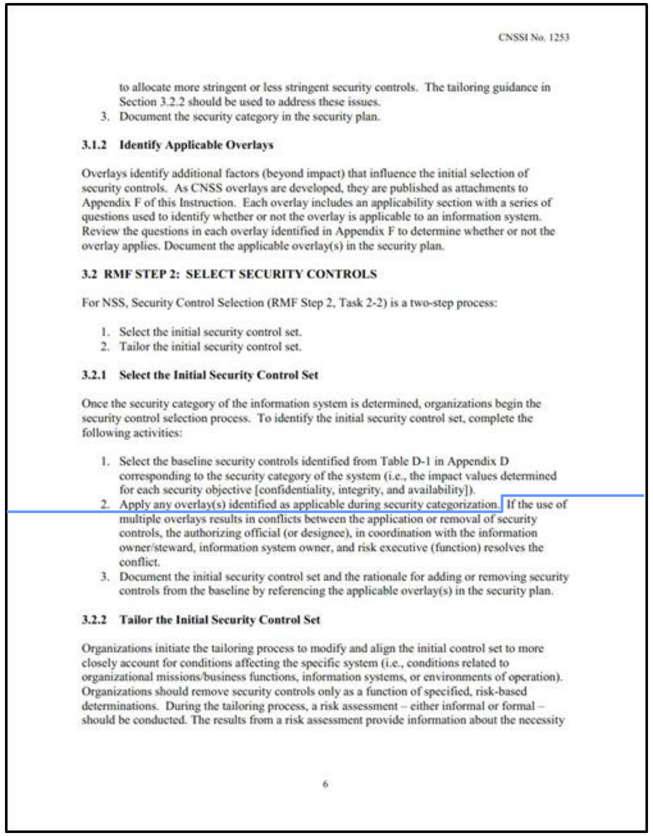
[5] Controlled interfaces protect information that is processed, stored, or transmitted on interconnected systems. That information should be considered when categorizing the controlled interface.

[6] For the confidentiality impact value, each organization should ensure that it categorizes specific information based on its potential worst case impact to i) its organization and ii) any and all other U.S. organizations with that specific information.

[7] As appropriate, supplement NIST SP 800-60 with organization-defined guidance.

5

Page 6



CNSSI No. 1253

to allocate more stringent or less stringent security controls. The tailoring guidance in Section 3.2.2 should be used to address these issues.

3. Document the security category in the security plan.

3.1.2 Identify Applicable Overlays

Overlays identify additional factors (beyond impact) that influence the initial selection of security controls. As CNSS overlays are developed, they are published as attachments to Appendix F of this Instruction. Each overlay includes an applicability section with a series of questions used to identify whether or not the overlay is applicable to an information system. Review the questions in each overlay identified in Appendix F to determine whether or not the overlay applies. Document the applicable overlay(s) in the security plan.

3.2 RMF STEP 2: SELECT SECURITY CONTROLS

For NSS, Security Control Selection (RMF Step 2, Task 2-2) is a two-step process:

1. Select the initial security control set.
2. Tailor the initial security control set.

3.2.1 Select the Initial Security Control Set

Once the security category of the information system is determined, organizations begin the security control selection process. To identify the initial security control set, complete the following activities:

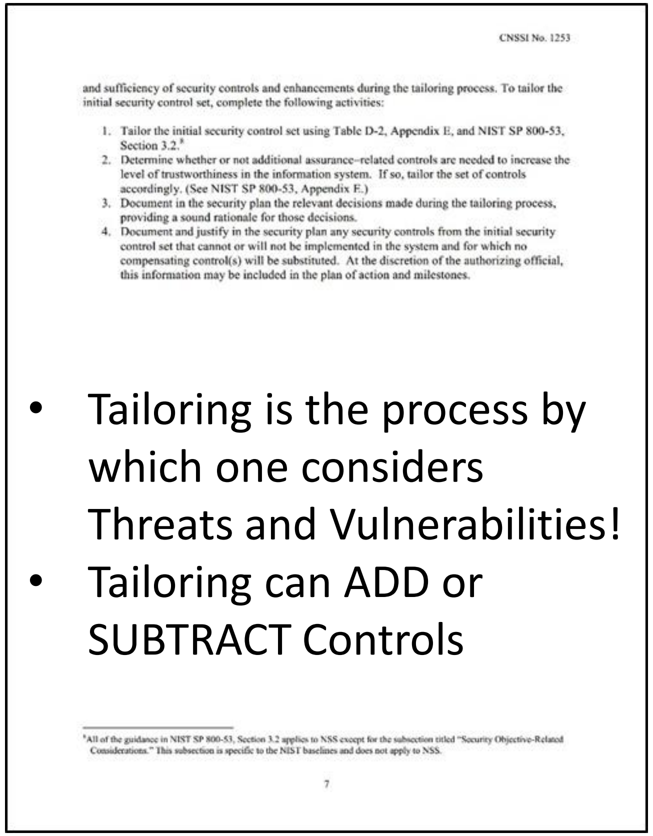
1. Select the baseline security controls identified from Table D-1 in Appendix D corresponding to the security category of the system (i.e., the impact values determined for each security objective [confidentiality, integrity, and availability]).
2. Apply any overlay(s) identified as applicable during security categorization. If the use of multiple overlays results in conflicts between the application or removal of security controls, the authorizing official (or designee), in coordination with the information owner/steward, information system owner, and risk executive (function) resolves the conflict.
3. Document the initial security control set and the rationale for adding or removing security controls from the baseline by referencing the applicable overlay(s) in the security plan.

3.2.2 Tailor the Initial Security Control Set

Organizations initiate the tailoring process to modify and align the initial control set to more closely account for conditions affecting the specific system (i.e., conditions related to organizational missions/business functions, information systems, or environments of operation). Organizations should remove security controls only as a function of specified, risk-based determinations. During the tailoring process, a risk assessment – either informal or formal – should be conducted. The results from a risk assessment provide information about the necessity

6

Page 7



CNSSI No. 1253

and sufficiency of security controls and enhancements during the tailoring process. To tailor the initial security control set, complete the following activities:

1. Tailor the initial security control set using Table D-2, Appendix E, and NIST SP 800-53, Section 3.2.[8]
2. Determine whether or not additional assurance–related controls are needed to increase the level of trustworthiness in the information system. If so, tailor the set of controls accordingly. (See NIST SP 800-53, Appendix E.)
3. Document in the security plan the relevant decisions made during the tailoring process, providing a sound rationale for those decisions.
4. Document and justify in the security plan any security controls from the initial security control set that cannot or will not be implemented in the system and for which no compensating control(s) will be substituted. At the discretion of the authorizing official, this information may be included in the plan of action and milestones.

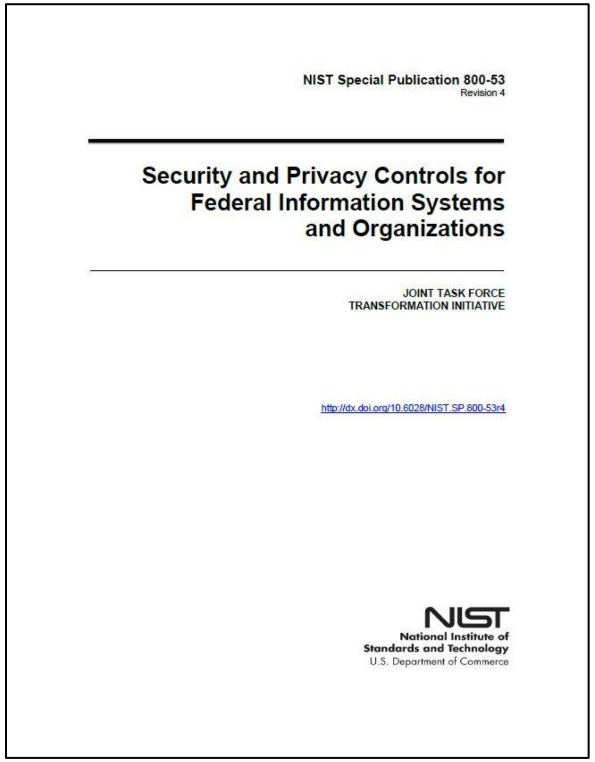
- Tailoring is the process by which one considers Threats and Vulnerabilities!
- Tailoring can ADD or SUBTRACT Controls

[8] All of the guidance in NIST SP 800-53, Section 3.2 applies to NSS except for the subsection titled "Security Objective-Related Considerations." This subsection is specific to the NIST baselines and does not apply to NSS.

7

Recognize the Correct Answer When Told (5 Year Old Known Process that Fulfills Requirement)

800-53, A.K.A., MIL-STD-961E W/CH1,§3 REQUIREMENTS
800-53A, A.K.A., MIL-STD-961E W/CH1,§4 VERIFICATION



NIST Special Publication 800-53
Revision 4

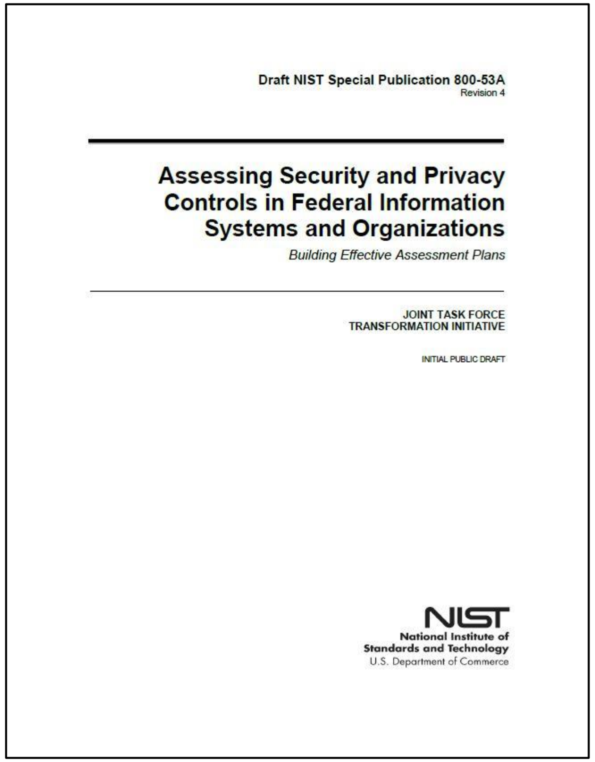
Security and Privacy Controls for
Federal Information Systems
and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

http://dx.doi.org/10.6028/NIST.SP.800-53r4

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

NIST SP 800-53r4
≈1,000 Requirements



Draft NIST Special Publication 800-53A
Revision 4

Assessing Security and Privacy
Controls in Federal Information
Systems and Organizations
Building Effective Assessment Plans

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

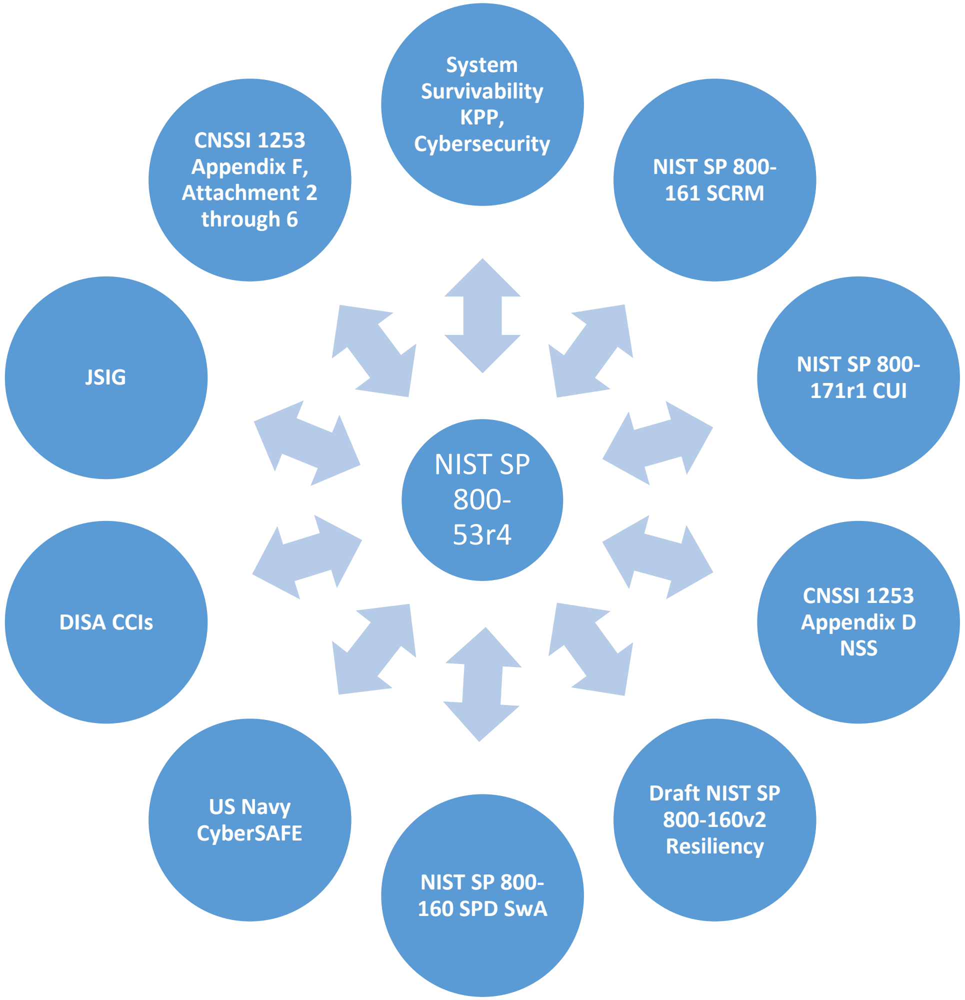
INITIAL PUBLIC DRAFT

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

NIST SP 800-53Ar4
≈4,000 Verification

CNSSI 1253 Selects ≈ LLL-311/MMM-403/HHH-478 Requirements
CNSSI 1253 w/Classified ≈ LLL-360/MMM-442/HHH-511 Requirements
CNSSI 1253 w/JSIG ≈ LLL-360/MMM-442/HHH-511 Requirements

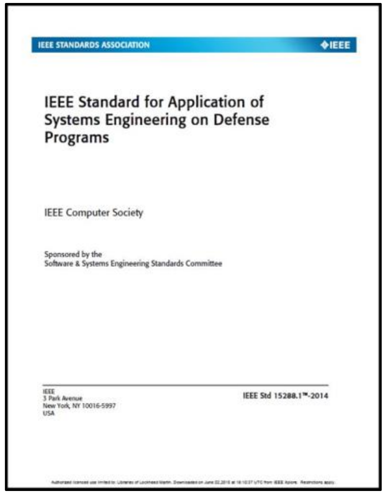
THE NIST SP 800-53r4 HUB AND SPOKES


NIST SP 800-53r4
System Survivability KPP, Cybersecurity
NIST SP 800-161 SCRM
NIST SP 800-171r1 CUI
CNSSI 1253 Appendix D NSS
Draft NIST SP 800-160v2 Resiliency
NIST SP 800-160 SPD SwA
US Navy CyberSAFE
DISA CCIs
JSIG
CNSSI 1253 Appendix F, Attachment 2 through 6

- NIST SP 800-53r4 is not a Requirements document in and of itself, BUT
- Many other documents call for the implementation of Controls and Control Enhancements, or
- Other Documents (CCIs) trace to its Controls and Control Enhancements
- Potential “Overlay’s” that give Owners “Confidence” in the System-of-Interest

Is there a trend here? We might want to do it the NIST SP 800-53r4 way!

IEEE STD 15288.1™-2014, IEEE STD 15288.2™-2014 and ISO/IEC/IEEE 15288:2015(E)


IEEE STANDARDS ASSOCIATION ◆IEEE

IEEE Standard for Application of Systems Engineering on Defense Programs

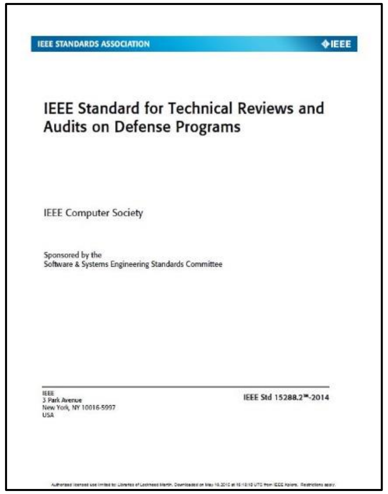
IEEE Computer Society

Sponsored by the
Software & Systems Engineering Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 15288.1™-2014

Authorized licensed use limited to: Libraries of Lockheed Martin. Downloaded on June 02,2015 at 18:10:37 UTC from IEEE Xplore. Restrictions apply.


IEEE STANDARDS ASSOCIATION ◆IEEE

IEEE Standard for Technical Reviews and Audits on Defense Programs

IEEE Computer Society

Sponsored by the
Software & Systems Engineering Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 15288.2™-2014

Authorized licensed use limited to: Libraries of Lockheed Martin. Downloaded on May 16,2015 at 15:10:10 UTC from IEEE Xplore. Restrictions apply.

INTERNATIONAL STANDARD

ISO/IEC/
IEEE
15288

First edition
2015-05-15

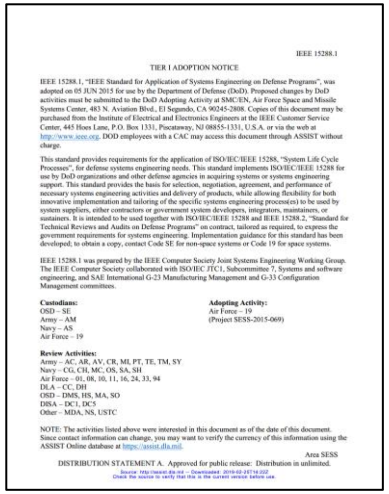
Systems and software engineering — System life cycle processes

Ingénierie des systèmes et du logiciel — Processus du cycle de vie du système

ISO IEC
◆IEEE

Reference number
ISO/IEC/IEEE 15288:2015(E)

© ISO/IEC 2015
© IEEE 2015


IEEE 15288.1

TIER I ADOPTION NOTICE

IEEE 15288.1, "IEEE Standard for Application of Systems Engineering on Defense Programs", was adopted on 05 JUN 2015 for use by the Department of Defense (DoD). Proposed changes by DoD activities must be submitted to the DoD Adopting Activity at SMC/EN, Air Force Space and Missile Systems Center, 483 N. Aviation Blvd., El Segundo, CA 90245-2808. Copies of this document may be purchased from the Institute of Electrical and Electronics Engineers at the IEEE Customer Service Center, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, U.S.A. or via the web at http://www.ieee.org. DOD employees with a CAC may access this document through ASSIST without charge.

This standard provides requirements for the application of ISO/IEC/IEEE 15288, "System Life Cycle Processes", for defense systems engineering needs. This standard implements ISO/IEC/IEEE 15288 for use by DoD organizations and other defense agencies in acquiring systems or systems engineering support. This standard provides the basis for selection, negotiation, agreement, and performance of necessary systems engineering activities and delivery of products, while allowing flexibility for both innovative implementation and tailoring of the specific systems engineering process(es) to be used by system suppliers, either contractors or government system developers, integrators, maintainers, or sustainers. It is intended to be used together with ISO/IEC/IEEE 15288 and IEEE 15288.2, "Standard for Technical Reviews and Audits on Defense Programs" on contract, tailored as required, to express the government requirements for systems engineering. Implementation guidance for this standard has been developed; to obtain a copy, contact Code SE for non-space systems or Code 19 for space systems.

IEEE 15288.1 was prepared by the IEEE Computer Society Joint Systems Engineering Working Group. The IEEE Computer Society collaborated with ISO/IEC JTC1, Subcommittee 7, Systems and software engineering, and SAE International G-23 Manufacturing Management and G-33 Configuration Management committees.

Custodians:
OSD – SE
Army – AM
Navy – AS
Air Force – 19

Adopting Activity:
Air Force – 19
(Project SESS-2015-069)

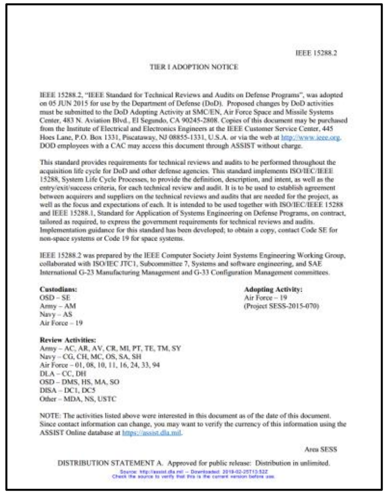
Review Activities:
Army – AC, AR, AV, CR, MI, PT, TE, TM, SY
Navy – CG, CH, MC, OS, SA, SH
Air Force – 01, 08, 10, 11, 16, 24, 33, 94
DLA – CC, DH
OSD – DMS, HS, MA, SO
DISA – DC1, DC5
Other – MDA, NS, USTC

NOTE: The activities listed above were interested in this document as of the date of this document. Since contact information can change, you may want to verify the currency of this information using the ASSIST Online database at https://assist.dla.mil.

Area SESS

DISTRIBUTION STATEMENT A. Approved for public release: Distribution in unlimited.

Source: http://assist.dla.mil -- Downloaded: 2019-02-25T14:22Z
Check the source to verify that this is the current version before use.


IEEE 15288.2

TIER I ADOPTION NOTICE

IEEE 15288.2, "IEEE Standard for Technical Reviews and Audits on Defense Programs", was adopted on 05 JUN 2015 for use by the Department of Defense (DoD). Proposed changes by DoD activities must be submitted to the DoD Adopting Activity at SMC/EN, Air Force Space and Missile Systems Center, 483 N. Aviation Blvd., El Segundo, CA 90245-2808. Copies of this document may be purchased from the Institute of Electrical and Electronics Engineers at the IEEE Customer Service Center, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, U.S.A. or via the web at http://www.ieee.org. DOD employees with a CAC may access this document through ASSIST without charge.

This standard provides requirements for technical reviews and audits to be performed throughout the acquisition life cycle for DoD and other defense agencies. This standard implements ISO/IEC/IEEE 15288, System Life Cycle Processes, to provide the definition, description, and intent, as well as the entry/exit/success criteria, for each technical review and audit. It is to be used to establish agreement between acquirers and suppliers on the technical reviews and audits that are needed for the project, as well as the focus and expectations of each. It is intended to be used together with ISO/IEC/IEEE 15288 and IEEE 15288.1, Standard for Application of Systems Engineering on Defense Programs, on contract, tailored as required, to express the government requirements for technical reviews and audits. Implementation guidance for this standard has been developed; to obtain a copy, contact Code SE for non-space systems or Code 19 for space systems.

IEEE 15288.2 was prepared by the IEEE Computer Society Joint Systems Engineering Working Group, collaborated with ISO/IEC JTC1, Subcommittee 7, Systems and software engineering, and SAE International G-23 Manufacturing Management and G-33 Configuration Management committees.

Custodians:
OSD – SE
Army – AM
Navy – AS
Air Force – 19

Adopting Activity:
Air Force – 19
(Project SESS-2015-070)

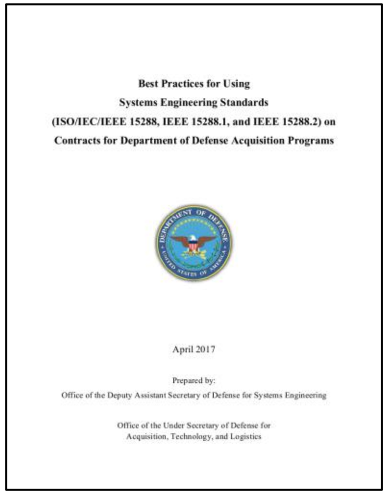
Review Activities:
Army – AC, AR, AV, CR, MI, PT, TE, TM, SY
Navy – CG, CH, MC, OS, SA, SH
Air Force – 01, 08, 10, 11, 16, 24, 33, 94
DLA – CC, DH
OSD – DMS, HS, MA, SO
DISA – DC1, DC5
Other – MDA, NS, USTC

NOTE: The activities listed above were interested in this document as of the date of this document. Since contact information can change, you may want to verify the currency of this information using the ASSIST Online database at https://assist.dla.mil.

Area SESS

DISTRIBUTION STATEMENT A. Approved for public release: Distribution in unlimited.

Source: http://assist.dla.mil -- Downloaded: 2019-02-25T13:52Z
Check the source to verify that this is the current version before use.


Best Practices for Using Systems Engineering Standards (ISO/IEC/IEEE 15288, IEEE 15288.1, and IEEE 15288.2) on Contracts for Department of Defense Acquisition Programs

April 2017

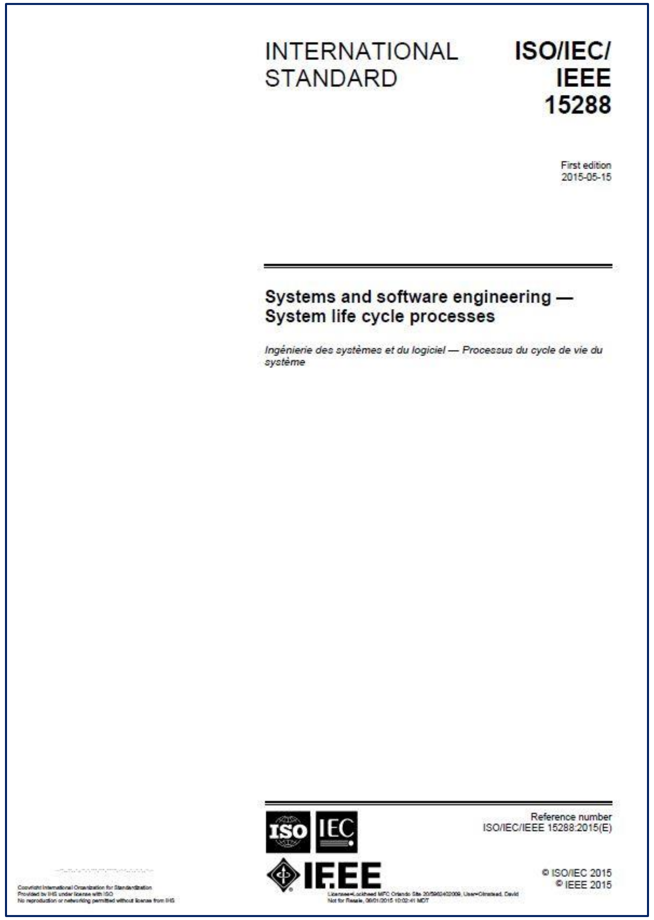
Prepared by:
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

Office of the Under Secretary of Defense for
Acquisition, Technology, and Logistics

- These standards addresses the needs of the defense community with respect to the incorporation, implementation, and execution of Systems Engineering
- IEEE Std 15288.1-2014 & 15288.2-2014 implement ISO/IEC/IEEE 15288 for application on defense programs
  - See the Tier I Adoption Notices
- DoD provides "Best Practices for using Systems Engineering Standards"
  - It notes the Tier I Adoption Notices and the three Standards for application
  - Defense-specific language and terminology to ensure the correct application of acquirer-supplier requirements for the DoD Acquisition Life Cycle
  - Systems Engineering, and Technical Reviews and Audits

Defense Program Systems Engineering; Tier I Adoption Notices and DoD Best Practices

ISO/IEC/IEEE 15288-2015(E) (ILLUSTRATIVE SAMPLE)



INTERNATIONAL STANDARD

ISO/IEC/
IEEE
15288

First edition
2015-05-15

Systems and software engineering — System life cycle processes

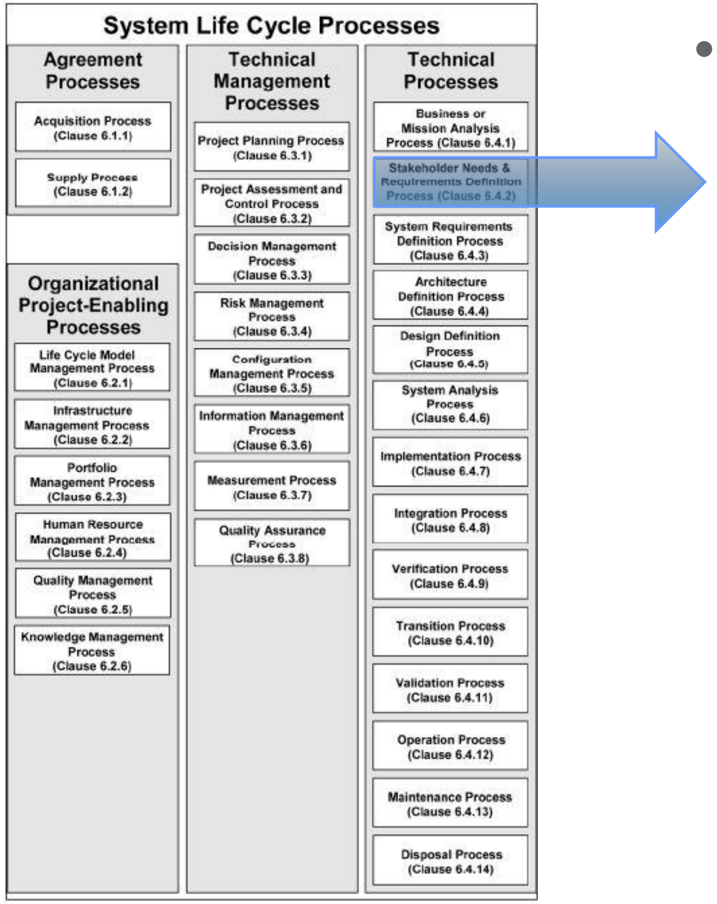
Ingénierie des systèmes et du logiciel — Processus du cycle de vie du système

Reference number
ISO/IEC/IEEE 15288:2015(E)

- §6.4.2 Stakeholder Needs and Requirements Definition Process
  - **The purpose of the Stakeholder Needs and Requirements Definition process is to define the stakeholder requirements for a system that can provide the capabilities needed by users and other stakeholders in a defined environment.**
    - Define Stakeholder Need includes: “Understanding stakeholder needs for the minimum security and privacy requirements necessary for the operational environment minimizes the potential for disruption in plans, schedules, and performance.”
    - Preview – Detail is added by NIST SP 800-160v1, Systems Security Engineering

The DoD Defined System Life Cycle Process Requirement

ISO/IEC/IEEE 15288-2015
THE REQUIREMENTS ENGINEER EARLY IN THE DEVELOPMENT



System Life Cycle Processes

Agreement Processes
- Acquisition Process (Clause 6.1.1)
- Supply Process (Clause 6.1.2)

Organizational Project-Enabling Processes
- Life Cycle Model Management Process (Clause 6.2.1)
- Infrastructure Management Process (Clause 6.2.2)
- Portfolio Management Process (Clause 6.2.3)
- Human Resource Management Process (Clause 6.2.4)
- Quality Management Process (Clause 6.2.5)
- Knowledge Management Process (Clause 6.2.6)

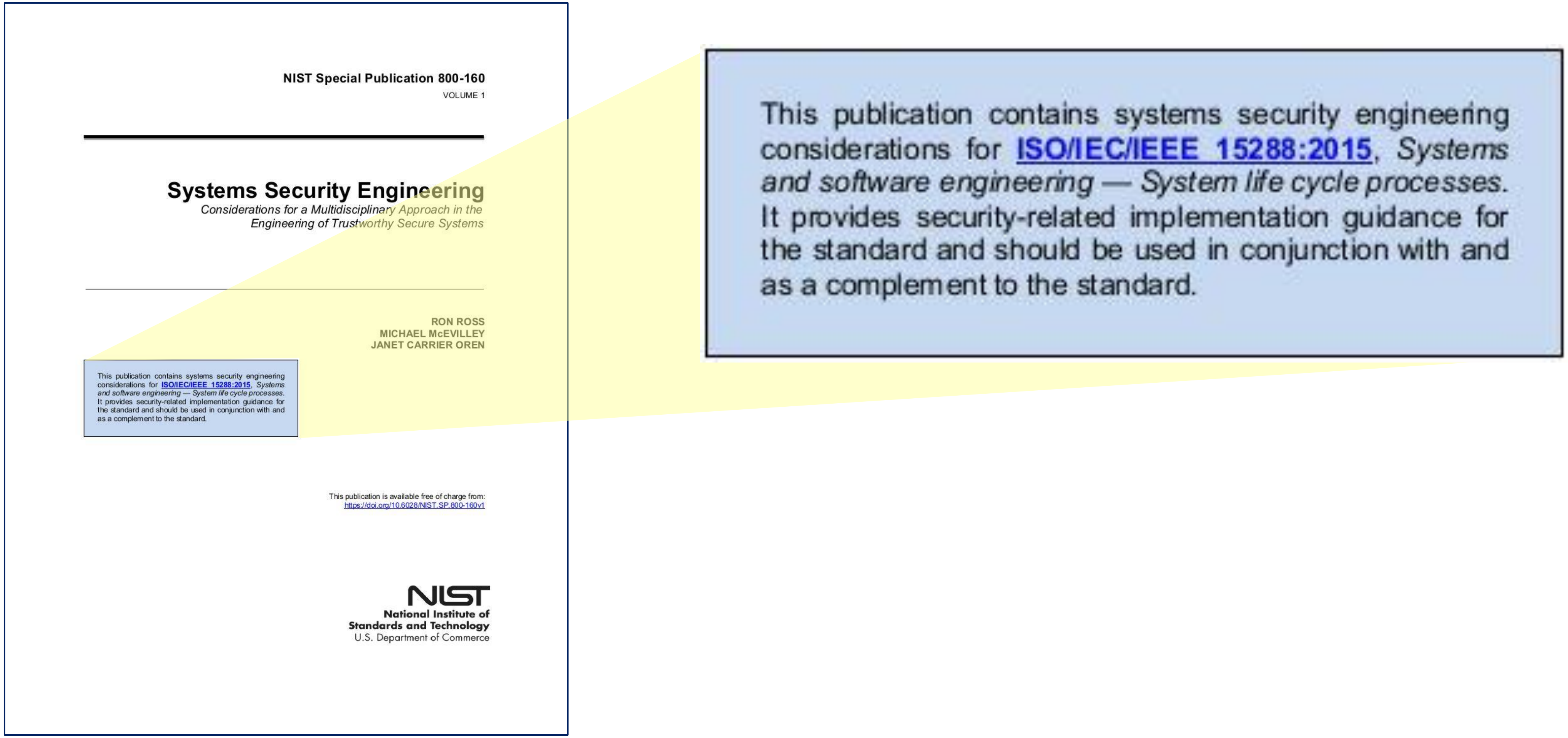
Technical Management Processes
- Project Planning Process (Clause 6.3.1)
- Project Assessment and Control Process (Clause 6.3.2)
- Decision Management Process (Clause 6.3.3)
- Risk Management Process (Clause 6.3.4)
- Configuration Management Process (Clause 6.3.5)
- Information Management Process (Clause 6.3.6)
- Measurement Process (Clause 6.3.7)
- Quality Assurance Process (Clause 6.3.8)

Technical Processes
- Business or Mission Analysis Process (Clause 6.4.1)
- Stakeholder Needs & Requirements Definition Process (Clause 6.4.2)
- System Requirements Definition Process (Clause 6.4.3)
- Architecture Definition Process (Clause 6.4.4)
- Design Definition Process (Clause 6.4.5)
- System Analysis Process (Clause 6.4.6)
- Implementation Process (Clause 6.4.7)
- Integration Process (Clause 6.4.8)
- Verification Process (Clause 6.4.9)
- Transition Process (Clause 6.4.10)
- Validation Process (Clause 6.4.11)
- Operation Process (Clause 6.4.12)
- Maintenance Process (Clause 6.4.13)
- Disposal Process (Clause 6.4.14)

- **§6.4.2 Stakeholder Needs and Requirements Definition Process**
  - **6.4.2.3 Activities and tasks**
    - Note Some stakeholders have interests that oppose the system or oppose each other. When the stakeholder interests oppose each other, but do not oppose the system, this process is intended to gain consensus among the stakeholder classes to establish a common set of acceptable requirements
    - b) Define Stakeholder Needs.
      - 1) Define context of use within the concept of operations and the preliminary life cycle concepts
      - 2) Identify stakeholder needs
      - 3) Prioritize and down-select needs
      - 4) Define the stakeholder needs and rationale

Position within the Technical Processes

NIST SP 800-160v1 IS PER ISO/IEC/IEEE 15288:2015(E)



NIST Special Publication 800-160
VOLUME 1

Systems Security Engineering
Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

RON ROSS
MICHAEL McEVILLEY
JANET CARRIER OREN

This publication contains systems security engineering considerations for ISO/IEC/IEEE 15288:2015, *Systems and software engineering — System life cycle processes.* It provides security-related implementation guidance for the standard and should be used in conjunction with and as a complement to the standard.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-160v1

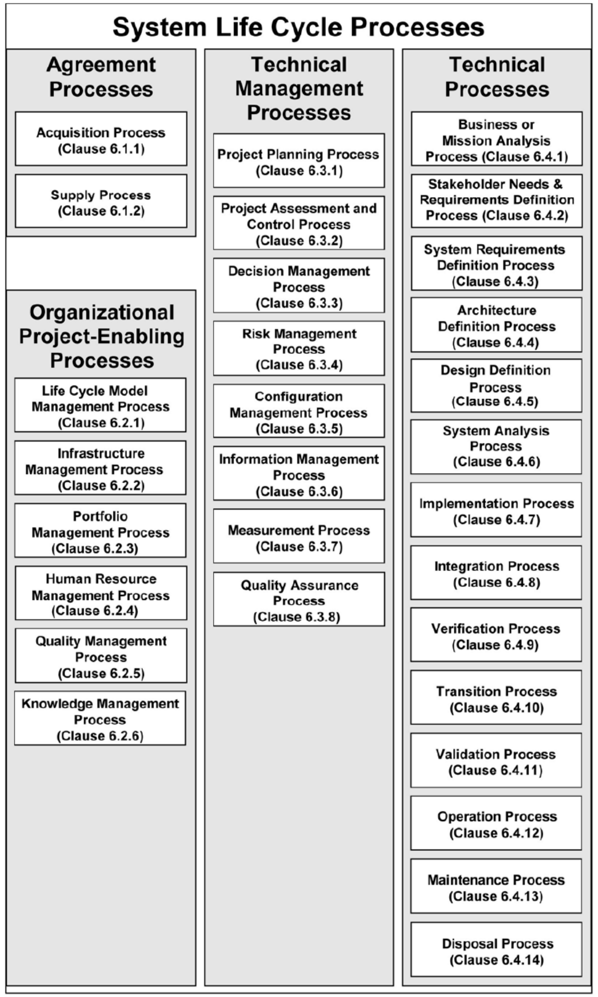
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

This publication contains systems security engineering considerations for ISO/IEC/IEEE 15288:2015, *Systems and software engineering — System life cycle processes.* It provides security-related implementation guidance for the standard and should be used in conjunction with and as a complement to the standard.

NIST SP 800-160v1 is a ISO/IEC/IEEE 15288:2015(E) Security VIEWPOINT

ISO/IEC/IEEE 15288:2015(E), SYSTEMS AND SOFTWARE ENGINEERING – SYSTEM LIFE CYCLE PROCESSES

ISO/IEC/IEEE 15288



System Life Cycle Processes

Agreement Processes
- Acquisition Process (Clause 6.1.1)
- Supply Process (Clause 6.1.2)

Organizational Project-Enabling Processes
- Life Cycle Model Management Process (Clause 6.2.1)
- Infrastructure Management Process (Clause 6.2.2)
- Portfolio Management Process (Clause 6.2.3)
- Human Resource Management Process (Clause 6.2.4)
- Quality Management Process (Clause 6.2.5)
- Knowledge Management Process (Clause 6.2.6)

Technical Management Processes
- Project Planning Process (Clause 6.3.1)
- Project Assessment and Control Process (Clause 6.3.2)
- Decision Management Process (Clause 6.3.3)
- Risk Management Process (Clause 6.3.4)
- Configuration Management Process (Clause 6.3.5)
- Information Management Process (Clause 6.3.6)
- Measurement Process (Clause 6.3.7)
- Quality Assurance Process (Clause 6.3.8)

Technical Processes
- Business or Mission Analysis Process (Clause 6.4.1)
- Stakeholder Needs & Requirements Definition Process (Clause 6.4.2)
- System Requirements Definition Process (Clause 6.4.3)
- Architecture Definition Process (Clause 6.4.4)
- Design Definition Process (Clause 6.4.5)
- System Analysis Process (Clause 6.4.6)
- Implementation Process (Clause 6.4.7)
- Integration Process (Clause 6.4.8)
- Verification Process (Clause 6.4.9)
- Transition Process (Clause 6.4.10)
- Validation Process (Clause 6.4.11)
- Operation Process (Clause 6.4.12)
- Maintenance Process (Clause 6.4.13)
- Disposal Process (Clause 6.4.14)

NIST SP 800-160 System Life Cycle Processes

3.1 AGREEMENT PROCESSES

3.1.1 Acquisition Process
3.1.2 Supply Process

3.2 ORGANIZATIONAL PROJECT-ENABLING PROCESSES

3.2.1 Life Cycle Model Management Process
3.2.2 Infrastructure Management Process
3.2.3 Portfolio Management Process
3.2.4 Human Resource Management Process
3.2.5 Quality Management Process
3.2.6 Knowledge Management Process

3.3 TECHNICAL MANAGEMENT PROCESSES

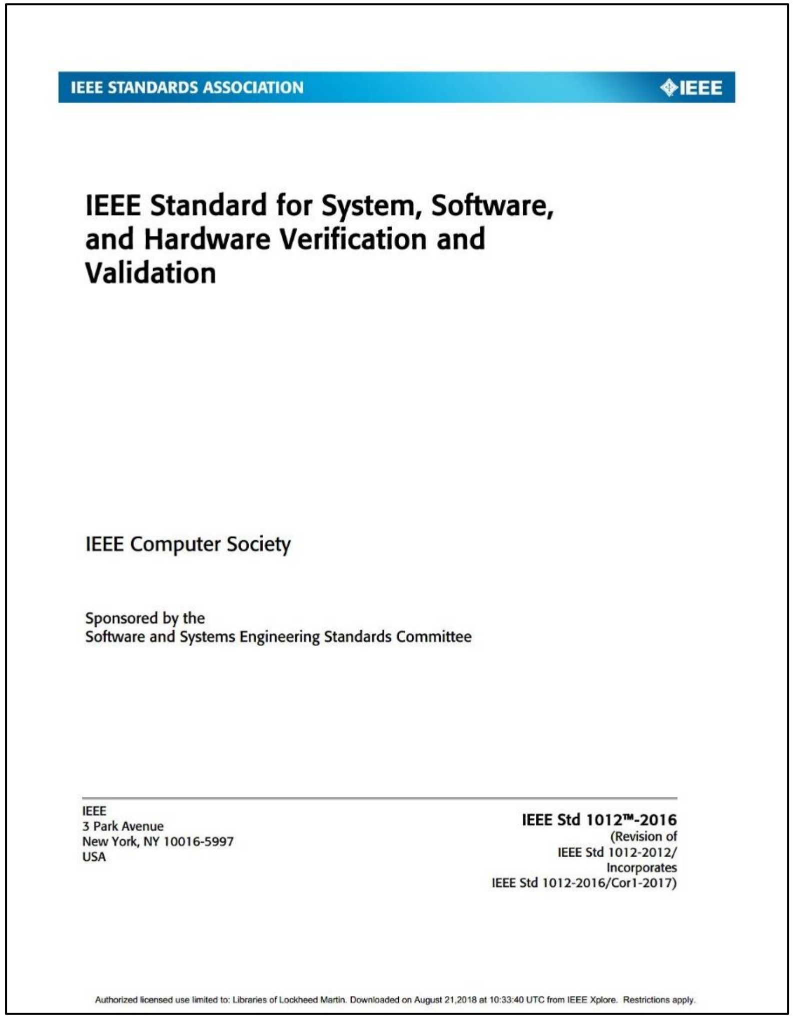
3.3.1 Project Planning Process
3.3.2 Project Assessment and Control Process
3.3.3 Decision Management Process
3.3.4 Risk Management Process
3.3.5 Configuration Management Process
3.3.6 Information Management Process
3.3.7 Measurement Process
3.3.8 Quality Assurance Process

3.4 TECHNICAL PROCESSES

3.4.1 Business or Mission Analysis Process
3.4.2 Stakeholder Needs and Requirements Definition Process
3.4.3 System Requirements Definition Process
3.4.4 Architecture Definition Process
3.4.5 Design Definition Process
3.4.6 System Analysis Process
3.4.7 Implementation Process
3.4.8 Integration Process
3.4.9 Verification Process
3.4.10 Transition Process
3.4.11 Validation Process
3.4.12 Operation Process
3.4.13 Maintenance Process
3.4.14 Disposal Process

Change the §6 number in ISO/IEC/IEEE to §3 in NIST SP 800-160 and the section numbering is in alignment

IEEE STD 1012™-2016



IEEE STANDARDS ASSOCIATION ◆IEEE

IEEE Standard for System, Software, and Hardware Verification and Validation

IEEE Computer Society

Sponsored by the
Software and Systems Engineering Standards Committee

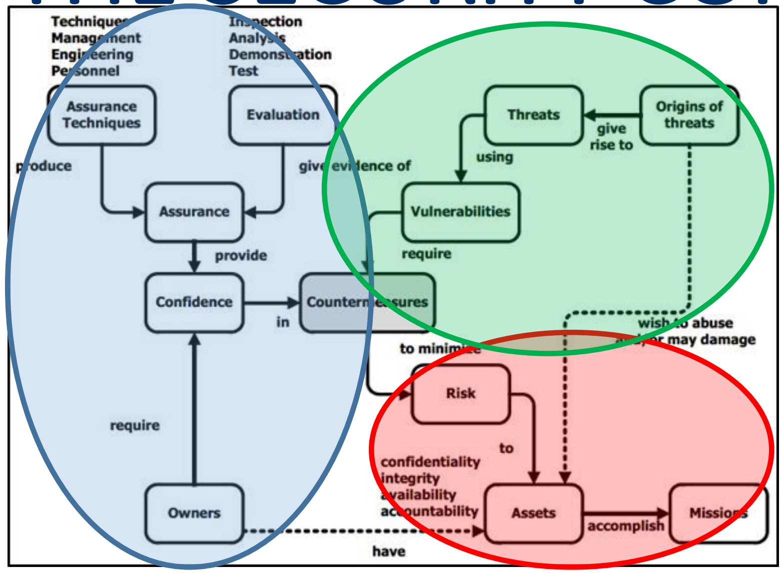
IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 1012™-2016
(Revision of
IEEE Std 1012-2012/
Incorporates
IEEE Std 1012-2016/Cor1-2017)

- Verification and validation (V&V) processes are used to determine whether the development products of a given activity conform to the requirements of that activity and whether the product satisfies its intended use and user needs.
- V&V life cycle process requirements are specified for different integrity levels.
- The scope of V&V processes encompasses systems, software, and hardware, and it includes their interfaces.
- This standard applies to systems, software, and hardware being developed, maintained, or reused (legacy, commercial off-the-shelf [COTS], non-developmental items).
- The term software also includes firmware and microcode, and each of the terms system, software, and hardware includes documentation.
- V&V processes include the analysis, evaluation, review, inspection, assessment, and testing of products.
- “Conducting system V&V as described in this V&V standard enables the V&V practitioner to claim full conformance with those two System Life Cycle [i.e., ISO/IEC/IEEE 15288:2015(E)] processes …”

§ 4. “…This V&V standard is a Conforming Instance of the Verification and Validation process in ISO/IEC/IEEE 15288:2015(E)”

IEEE STD 1012™-2016, (INFORMATIVE) FIGURE J.1 THE SECURITY CONTEXT OF THE SYSTEM



There are two (2) entrances to "Countermeasures"

- "Baseline" Assurance to give Owners Confidence in the System-of-Interest
- Threats that use Vulnerabilities and Require Countermeasures

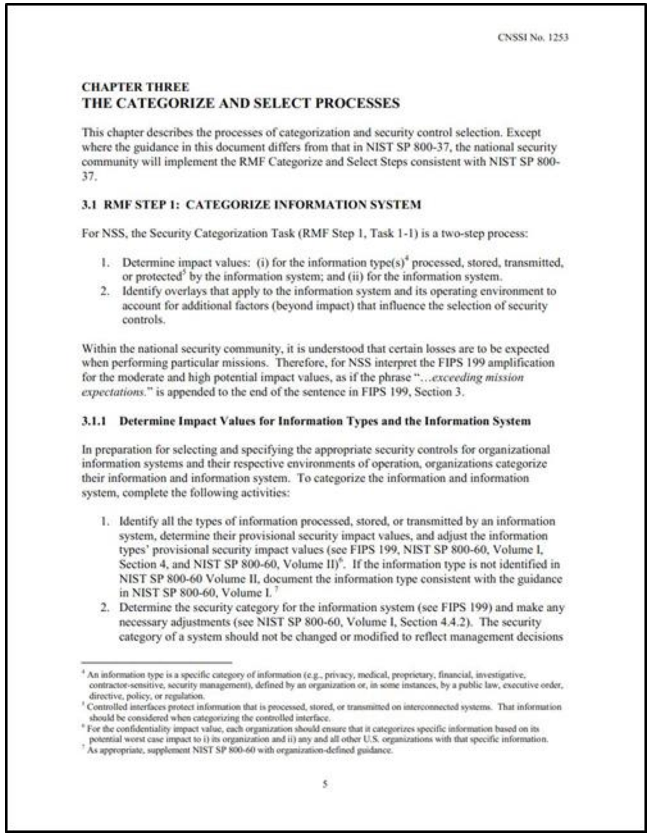
Both are "Mission Driven"

- One of the objectives of security analysis performed by the V&V effort is to verify that the system-required threat controls and safeguards are correctly implemented and to validate that they provide the desired levels of protection of system vulnerabilities. The other objective is to verify that there is a process for describing the system, software, and hardware process security.
- A system should consider different security issues in each phase of the life cycle because the system owner may change as the product evolves. The V&V security analysis should consider:
  - The context of the system (e.g., the development process and environment, the final operational environment, organization structures and management policy, operational and maintenance personnel roles, interfaces with other external systems or support systems);
  - The system of interest and its elements, threats, vulnerabilities, and countermeasures;
  - Tradeoffs between techniques, operations, and management to address security requirements.
  - Identification of threats. These threats may be natural (e.g., inclement weather, earthquakes), human (e.g., unintended or malicious), or environmental (e.g., chemical leak, power loss).

Cybersecurity (i.e., Security Context) is "Built Into" Verification and Validation

CNSSI 1253, 20140327
CHAPTER 3, THE CATEGORIZE AND SELECT PROCESSES

Page 5



CNSSI No. 1253

CHAPTER THREE
THE CATEGORIZE AND SELECT PROCESSES

This chapter describes the processes of categorization and security control selection. Except where the guidance in this document differs from that in NIST SP 800-37, the national security community will implement the RMF Categorize and Select Steps consistent with NIST SP 800-37.

3.1 RMF STEP 1: CATEGORIZE INFORMATION SYSTEM

For NSS, the Security Categorization Task (RMF Step 1, Task 1-1) is a two-step process:

1. Determine impact values: (i) for the information type(s)[4] processed, stored, transmitted, or protected[5] by the information system; and (ii) for the information system.
2. Identify overlays that apply to the information system and its operating environment to account for additional factors (beyond impact) that influence the selection of security controls.

Within the national security community, it is understood that certain losses are to be expected when performing particular missions. Therefore, for NSS interpret the FIPS 199 amplification for the moderate and high potential impact values, as if the phrase "…*exceeding mission expectations.*" is appended to the end of the sentence in FIPS 199, Section 3.

3.1.1 Determine Impact Values for Information Types and the Information System

In preparation for selecting and specifying the appropriate security controls for organizational information systems and their respective environments of operation, organizations categorize their information and information system. To categorize the information and information system, complete the following activities:

1. Identify all the types of information processed, stored, or transmitted by an information system, determine their provisional security impact values, and adjust the information types' provisional security impact values (see FIPS 199, NIST SP 800-60, Volume I, Section 4, and NIST SP 800-60, Volume II)[6]. If the information type is not identified in NIST SP 800-60 Volume II, document the information type consistent with the guidance in NIST SP 800-60, Volume I. [7]
2. Determine the security category for the information system (see FIPS 199) and make any necessary adjustments (see NIST SP 800-60, Volume I, Section 4.4.2). The security category of a system should not be changed or modified to reflect management decisions

[4] An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor-sensitive, security management), defined by an organization or, in some instances, by a public law, executive order, directive, policy, or regulation.

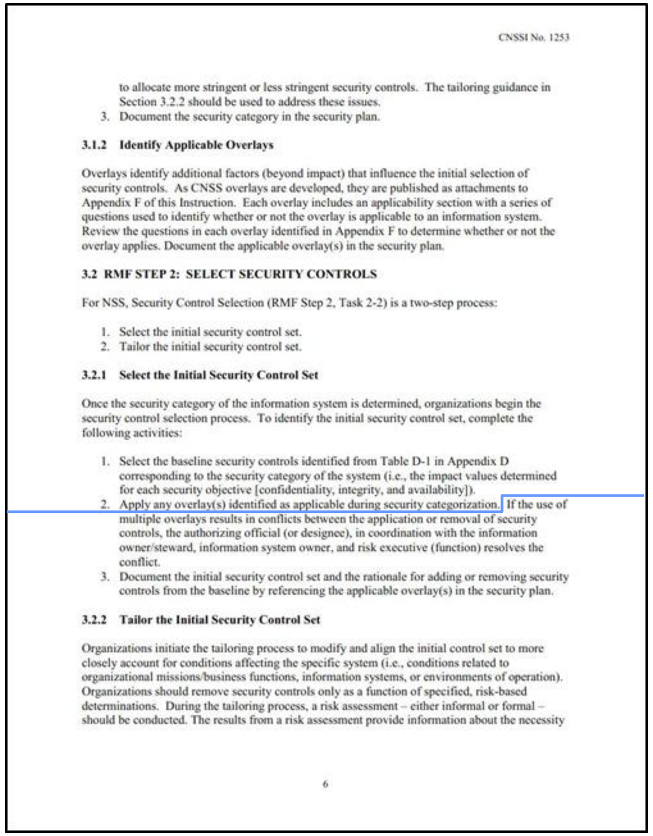
[5] Controlled interfaces protect information that is processed, stored, or transmitted on interconnected systems. That information should be considered when categorizing the controlled interface.

[6] For the confidentiality impact value, each organization should ensure that it categorizes specific information based on its potential worst case impact to i) its organization and ii) any and all other U.S. organizations with that specific information.

[7] As appropriate, supplement NIST SP 800-60 with organization-defined guidance.

5

Page 6



CNSSI No. 1253

to allocate more stringent or less stringent security controls. The tailoring guidance in Section 3.2.2 should be used to address these issues.

3. Document the security category in the security plan.

3.1.2 Identify Applicable Overlays

Overlays identify additional factors (beyond impact) that influence the initial selection of security controls. As CNSS overlays are developed, they are published as attachments to Appendix F of this Instruction. Each overlay includes an applicability section with a series of questions used to identify whether or not the overlay is applicable to an information system. Review the questions in each overlay identified in Appendix F to determine whether or not the overlay applies. Document the applicable overlay(s) in the security plan.

3.2 RMF STEP 2: SELECT SECURITY CONTROLS

For NSS, Security Control Selection (RMF Step 2, Task 2-2) is a two-step process:

1. Select the initial security control set.
2. Tailor the initial security control set.

3.2.1 Select the Initial Security Control Set

Once the security category of the information system is determined, organizations begin the security control selection process. To identify the initial security control set, complete the following activities:

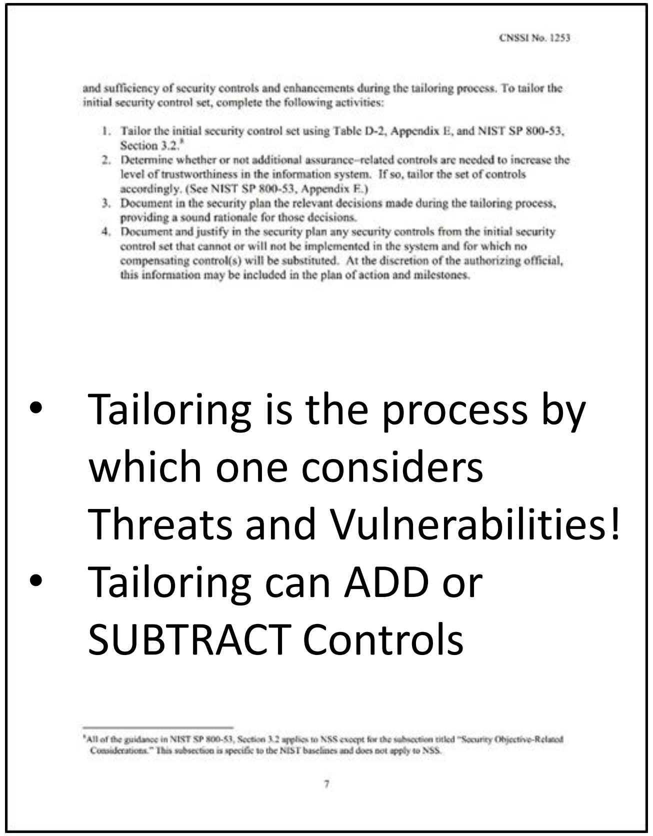
1. Select the baseline security controls identified from Table D-1 in Appendix D corresponding to the security category of the system (i.e., the impact values determined for each security objective [confidentiality, integrity, and availability]).
2. Apply any overlay(s) identified as applicable during security categorization. If the use of multiple overlays results in conflicts between the application or removal of security controls, the authorizing official (or designee), in coordination with the information owner/steward, information system owner, and risk executive (function) resolves the conflict.
3. Document the initial security control set and the rationale for adding or removing security controls from the baseline by referencing the applicable overlay(s) in the security plan.

3.2.2 Tailor the Initial Security Control Set

Organizations initiate the tailoring process to modify and align the initial control set to more closely account for conditions affecting the specific system (i.e., conditions related to organizational missions/business functions, information systems, or environments of operation). Organizations should remove security controls only as a function of specified, risk-based determinations. During the tailoring process, a risk assessment – either informal or formal – should be conducted. The results from a risk assessment provide information about the necessity

6

Page 7



CNSSI No. 1253

and sufficiency of security controls and enhancements during the tailoring process. To tailor the initial security control set, complete the following activities:

1. Tailor the initial security control set using Table D-2, Appendix E, and NIST SP 800-53, Section 3.2.[8]
2. Determine whether or not additional assurance–related controls are needed to increase the level of trustworthiness in the information system. If so, tailor the set of controls accordingly. (See NIST SP 800-53, Appendix E.)
3. Document in the security plan the relevant decisions made during the tailoring process, providing a sound rationale for those decisions.
4. Document and justify in the security plan any security controls from the initial security control set that cannot or will not be implemented in the system and for which no compensating control(s) will be substituted. At the discretion of the authorizing official, this information may be included in the plan of action and milestones.

- Tailoring is the process by which one considers Threats and Vulnerabilities!
- Tailoring can ADD or SUBTRACT Controls

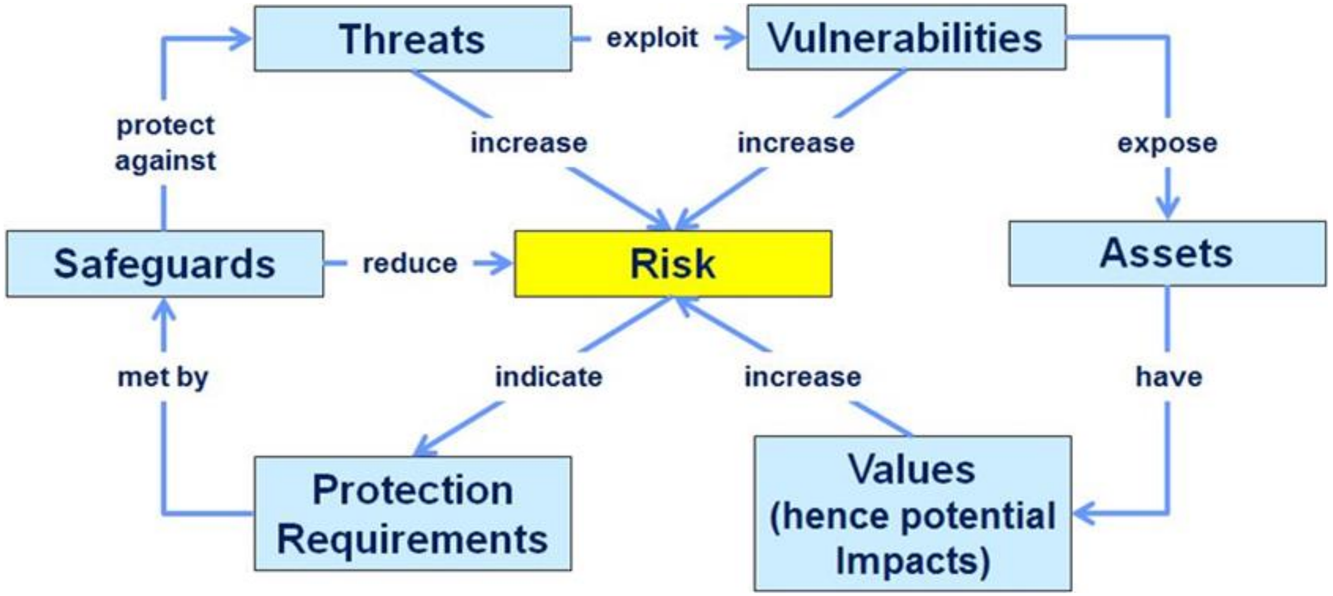
[8] All of the guidance in NIST SP 800-53, Section 3.2 applies to NSS except for the subsection titled "Security Objective-Related Considerations." This subsection is specific to the NIST baselines and does not apply to NSS.

7

Recognize the Correct Answer When Told (5 Year Old Known Process that Fulfills Requirement)

RELATIONSHIPS IN RISK MANAGEMENT MODEL

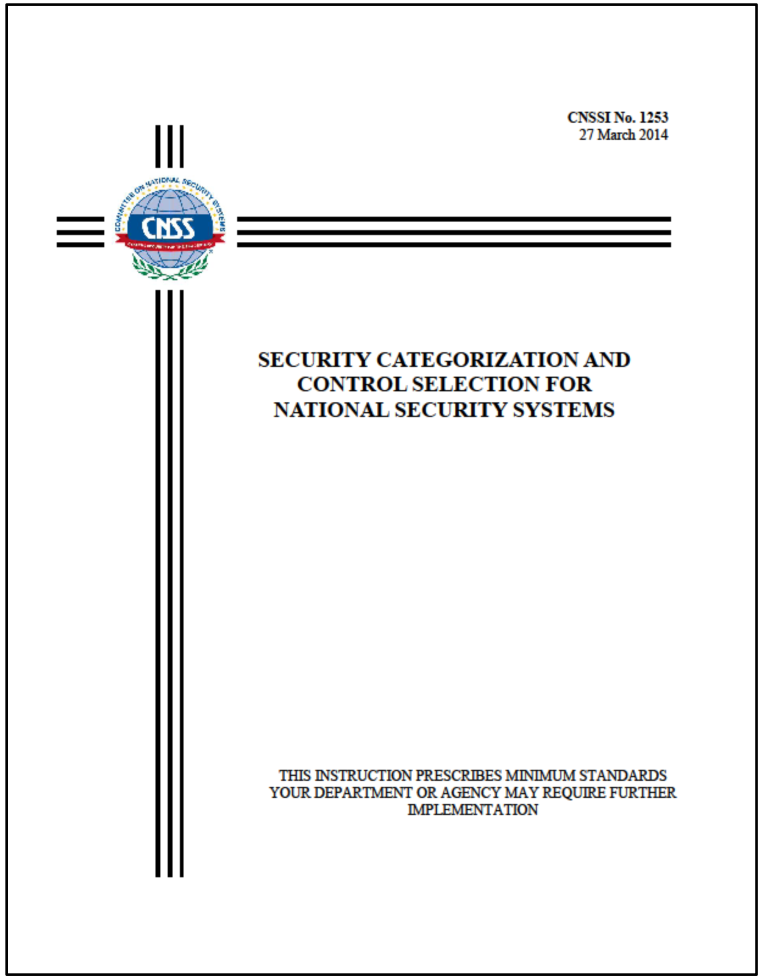
- ISO/IEC TR 13335-1:1996
- Information technology – Guidelines for the management of IT Security – Part 1: Concepts and models for IT Security
- Figure 4: Relationships in risk Management
- This can easily transform into IEEE Std 1012™-2016 Figure J.1



Changing Threats/Vulnerabilities = Never Ending Process (33 Year Old Model)

SOURCE DOCUMENTS

CNSSI 1253, 20140327

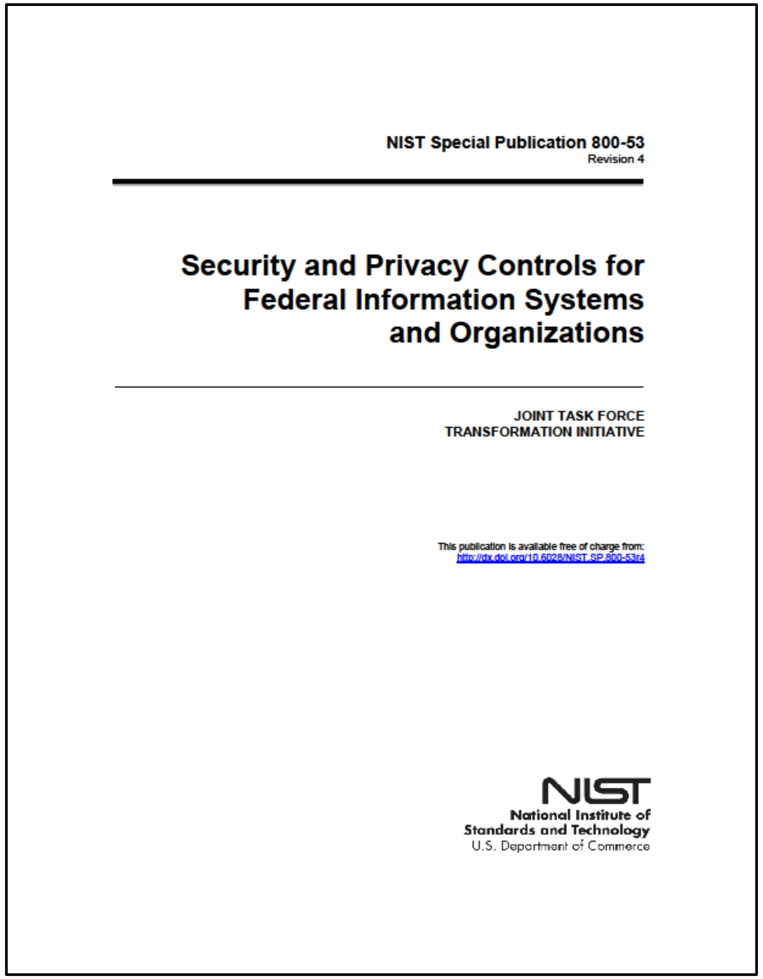


CNSSI No. 1253
27 March 2014

SECURITY CATEGORIZATION AND
CONTROL SELECTION FOR
NATIONAL SECURITY SYSTEMS

THIS INSTRUCTION PRESCRIBES MINIMUM STANDARDS
YOUR DEPARTMENT OR AGENCY MAY REQUIRE FURTHER
IMPLEMENTATION

NIST SP 800-53r4



NIST Special Publication 800-53
Revision 4

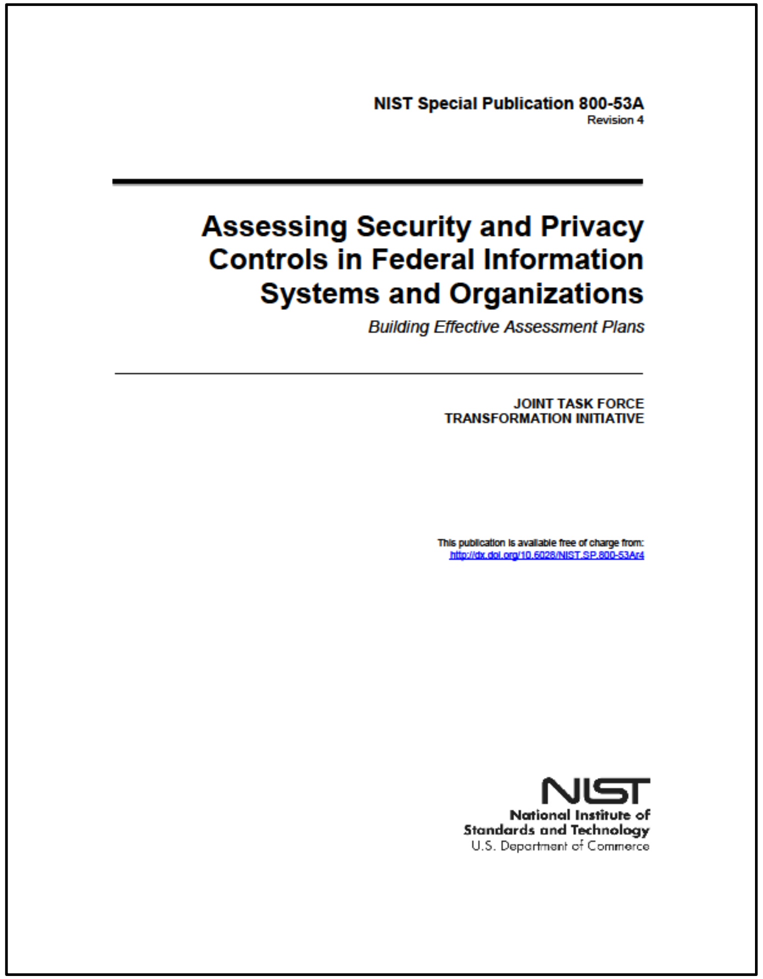
Security and Privacy Controls for
Federal Information Systems
and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

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

NIST SP 800-53Ar4



NIST Special Publication 800-53A
Revision 4

Assessing Security and Privacy
Controls in Federal Information
Systems and Organizations

Building Effective Assessment Plans

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

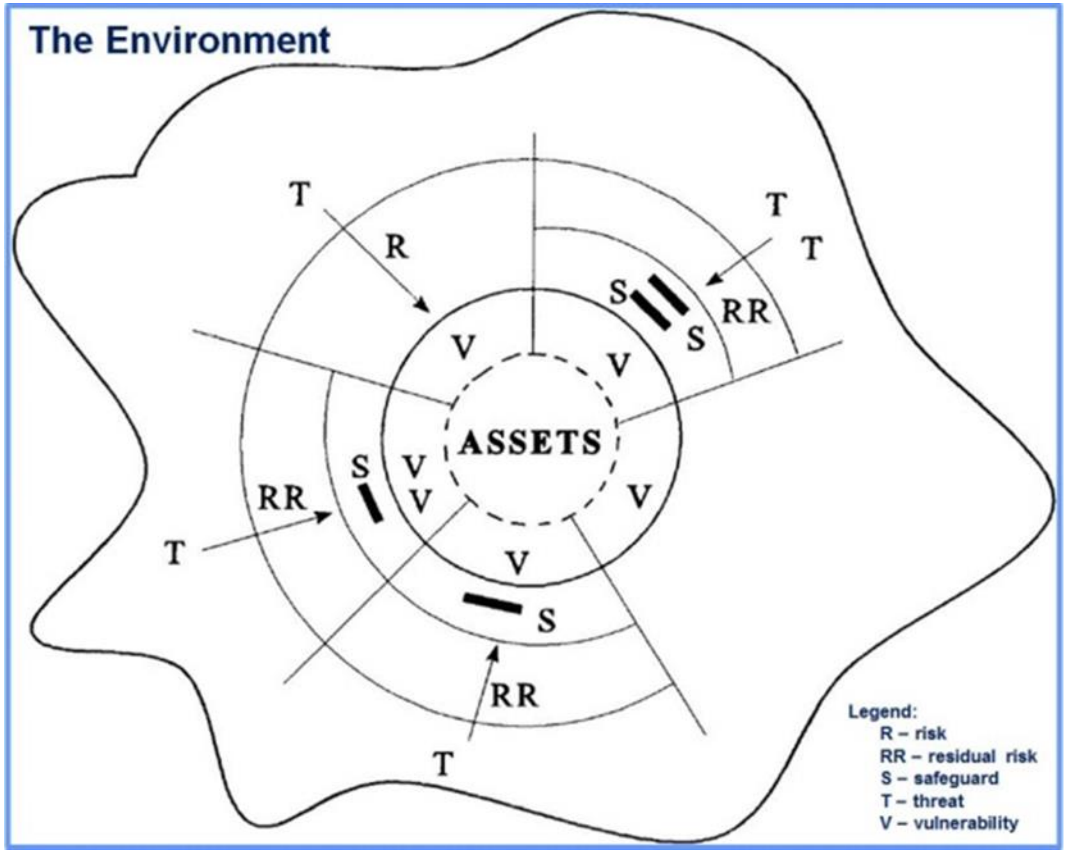
This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53Ar4

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

“Baseline” Assurance to give Owners “Confidence” in the System-of-Interest

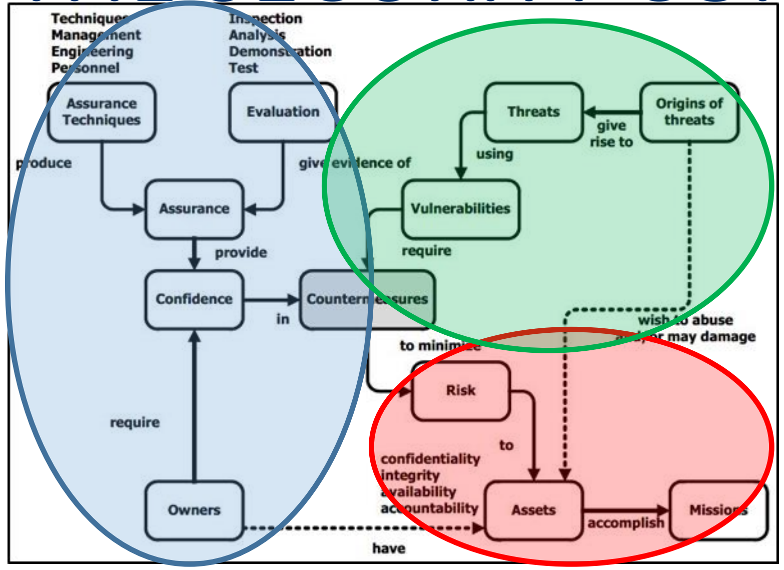
SECURITY ELEMENT RELATIONSHIPS MODEL

- ISO/IEC TR 13335-1:1996
- Information technology – Guidelines for the management of IT Security – Part 1: Concepts and models for IT Security
- Figure 3: Security Element Relationships
- A static representation; no indication as to the "safeguard" being "designed in" (i.e., Baseline) or "added on" (Threat / Vulnerability Analysis Process)
  - Is the "safeguard" part of the Baseline
  - Is the "safeguard" part of the Threat Vulnerability Analysis Process
  - Does not matter



Snap-shot in Time, "Initial Security Control Set" or "Tailored Initial Security Control Set" (33 Year Old Model)

IEEE STD 1012™-2016, (INFORMATIVE) FIGURE J.1 THE SECURITY CONTEXT OF THE SYSTEM



There are two (2) entrances to "Countermeasures"

- "Baseline" Assurance to give Owners Confidence in the System-of-Interest
- Threats that use Vulnerabilities and Require Countermeasures

Both are "Mission Driven"

- One of the objectives of security analysis performed by the V&V effort is to verify that the system-required threat controls and safeguards are correctly implemented and to validate that they provide the desired levels of protection of system vulnerabilities. The other objective is to verify that there is a process for describing the system, software, and hardware process security.
- A system should consider different security issues in each phase of the life cycle because the system owner may change as the product evolves. The V&V security analysis should consider:
  - The context of the system (e.g., the development process and environment, the final operational environment, organization structures and management policy, operational and maintenance personnel roles, interfaces with other external systems or support systems);
  - The system of interest and its elements, threats, vulnerabilities, and countermeasures;
  - Tradeoffs between techniques, operations, and management to address security requirements.
  - Identification of threats. These threats may be natural (e.g., inclement weather, earthquakes), human (e.g., unintended or malicious), or environmental (e.g., chemical leak, power loss).

Cybersecurity (i.e., Security Context) is "Built Into" Verification and Validation

LOCKHEED MARTIN