CYBERSECURITY THE SYSTEMS ENGINEERING WAY

20181001

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

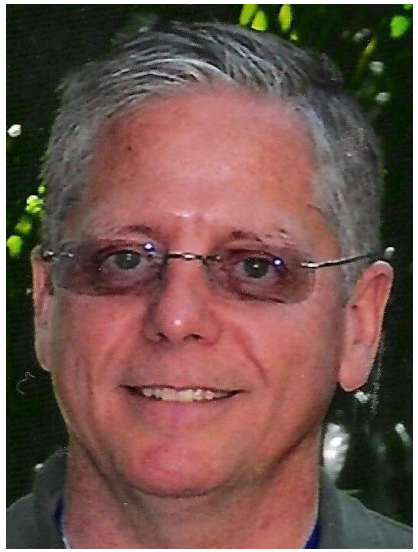
LOCKHEED MARTIN

SYSTEM SECURITY SYSTEMS ENGINEERING

MFC CYBER SECURITY

SYSTEMS ENGINEERING

PERMIT ME TO INTRODUCE MYSELF,



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

CONVINCE THE SYSTEMS SECURITY ENGINEERING COMMUNITY, CONTRACTOR PROGRAM MANAGEMENT, AND US GOVERNMENT PROGRAM OFFICE, AND

CONVINCE PIT SYSTEM / PIT AUTHORIZING OFFICIALS (AOS) / INFORMATION SYSTEM SECURITY MANAGERS (ISSMS) /SECURITY CONTROL ASSESSORS (SCAS) THAT

SYSTEMS SECURITY ENGINEERING IS THE ONLY AFFORDABLE OPTION FOR PIT SYSTEM / PIT CYBERSECURITY

BLUF

RMF, SYSTEMS SECURITY ENGINEERING AND DoD PIT SYSTEMS / PIT (ESSENTIAL REFERENCES)

- Risk Management Framework (RMF) is a set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization (ISO 31000:2009(E)§2.3)
- National Institute of Standards and Technology (NIST) Transformational Documents defined RMF:
  - **NIST SP 800-30, Guide for Conducting Risk Assessments;**
  - **NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach;**
  - **NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View;**
  - **NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations; and**
  - **NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans.**
- NIST also published Special Publication 800-160 (NIST SP 800-160v1) Systems Security Engineering; it is a Process View (defined by ISO/IEC/IEEE 15288:2015(E), Annex E Process Views)
- PIT (Platform Information Technology) and PIT Systems are hardware and software IT that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems (PIT System are a collection of PIT) (e.g., weapons and weapon systems, etc.)

I.E., Contractor DoD Developmental Product Line Systems Security Requirements Life Cycle

CORELATED ENCLAVE TO PIT SYSTEM / PIT WORK PRODUCTS

Enclave Work Products (Stove-Pipe)

- Cybersecurity Strategy
- System Security Plan (SSP) (RMS KS)
  - Ports, Protocols, & Services Management
  - DoD Security Control Set
  - System Authorization Boundary
- Continuous Monitoring Strategy (CMS) (NIST SP 800-137 ISCM)
- Security Assessment Plan (SAP)
- Security Assessment Report (SAR)
- Risk Assessment Report (RAR)
- Plan of Action and Milestones (POA&M)

PIT System / PIT Work Products (Integrated)

- PPP/PPIP at Appendix E (DoD CIO memo of 20151110 w/template)
- System Requirements Specification (SyRS), etc., flow-down Spec.
  - §2 Applicable Documents (Internal/External ICDs tied to §6.1 DoDAF SV-1, SV-3)
  - §3 Requirements (against HWCI/CSCI Critical Component from PPIP Appendix C) with System-of-Interest C-I-A & Overlays (from NIST SP 800-53r4 and associated CCIs)
  - §6.1 Intended Use (to include DoDAF OV-1 High-Level Operational Concept Graphic, DoDAF SV-1 Systems Interface Description, and SV-3 Systems-Systems Matrix)
- Cybersecurity Section of SEMP (Tier 1 and/or 2), SyRS §6.1 Intended Use (System-of-Interest Tier 3 Strategy) and PPIP
- TEMP Cybersecurity Section & SyRS (w/flow-down) §4 Verification
- SyRS (w/flow-down)§4 Verification Reports
- Pre MS-A & B Analysis Reports (Design Residual Risk) and Cybersecurity Section of DT&E/OT&E for Requirement Compliance
  - Note, the 15288/800-160 (§6.4.2.3e/§3.4.2 SN-5) Analyze Stakeholder Security Requirements Report "Defines" Design SySR Residual Risk for System-of-Interest
- Engineering Change Proposal (ECP) / Preplanned Product Improvement (P3I)

PIT Acquisition Systems Engineering Includes Enclave "Stove-Pipe" Work Products

CYBERSECURITY IN DoD ACQUISITION OF DEVELOPMENTAL CONFIGURATION ITEMS (I.E., PIT MATERIEL PROCUREMENT)

- Recognize the need for Security within the System-of-Interest (i.e., PIT) at MDD
- Include Cybersecurity (and other Security, e.g., AT, SwA, SCRM) with all the other System-of-Interest Requirements (System Survivability KPP)
- For National Security Systems (NSS a.k.a., weapons, etc.) execute CNSSI 1253 Chapter 3
- Between Alternative System Review (ASR) and System Requirements Review (SRR) resolve Competing and Conflicting Requirements (Required Requirements Engineering)
  - **Publish System-of-Interest System Requirements Specification (SyRS)**
  - **The Cybersecurity Competing and Conflicting Requirements Analysis Report Defines the System-of-Interest (SoI) "Residual Risk" and requires AO/ISSM Approval**
    - Milestone B Entrance Criteria (RMF Step 2+ (Select), vice waiting to RMF Step 5 (Authorize))
    - The SoI "Residual Risk" report is analogous to an Enclave Risk Assessment Report (RAR)
      - P3I or ECP addresses SoI Non-compliance (POA&M addresses Enclave vulnerabilities)
  - **All SyRS Requirements will be "Compliant" and "Verified" (SyRS §4 Verification)**
- Follow the normal DoD Acquisition Process to obtain a Compliant SoI

Built In Cybersecurity using Requirements Engineering is the only Affordable Solution

CONTINUE THE BRIEFING (NOT BRIEF) FOR THE DETAILS.

END OF BLUF

THE REACTIVE VS. PROACTIVE RISK APPETITE BASED ON TYPE OF CONSEQUENCES TOLERABLE CONSEQUENCE VS. INTOLERABLE CONSEQUENCE

WHAT IS THE ORGANIZATION RISK APPETITE

WHAT DOES IT TAKE TO GET A TRAFFIC LIGHT IN A "IF IT ISN'T BROKE DON'T FIX IT SOCIETY"?

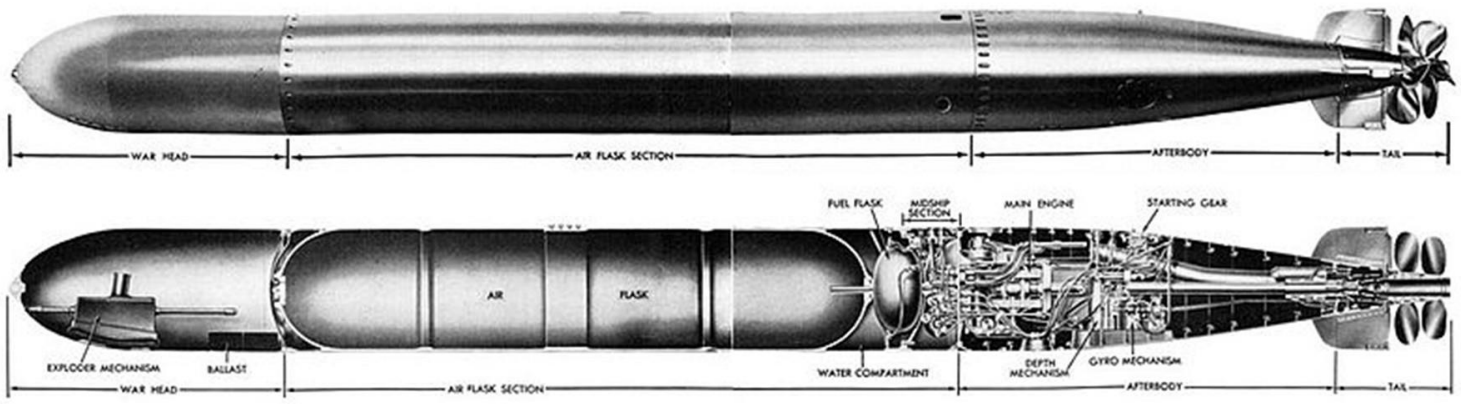
We "accept" the consequence that a minimum of 5 reportable crashes will occur (Reactive to "small" threat)

https://commons.wikimedia.org/wiki/File:Minor_traffic_accident_Memphis_TN_2013-08-03_001.jpg
By Thomas R Machnitzki (thomasmachnitzki.com) [GFDL (http://www.gnu.org/copyleft/fdl.html) or CC BY 3.0 (https://creativecommons.org/licenses/by/3.0)], from Wikimedia Commons

- **According to Part 4-Highway Traffic Signals, Warrant 7, Crash Experience (page 445), it takes five (5) or more reported crashes within a 12-month period and exceeding one of the traffic volume requirements to get a traffic light at an intersection**
  (US DOT, FHA Manual on Uniform Traffic Control Devices – MUTCD)
  - **A reactive risk society; if its not broken don't fix it!**

By US DOT Standard we only act on a "Documented" Problem

THE LAW OF UNINTENDED CONSEQUENCES; HOW US NAVY BuOrd COST LIVES IN WW II



- **It ran about 10 feet deeper than its depth setting**
- **The Magnetic exploder often caused premature firings.**
- **The contact exploder would fail.**
- **It tended to run in a circle and would strike the launching boat** (USS Tullibee, SS 284, was a confirmed fratricide)

Mark 14 torpedo's side view and interior mechanisms, published in "Torpedoes Mark 14 and 23 Types, OP 635", March 24, 1945, Public Domain image.
The *Bureau of Ordnance* (BuOrd) was the U.S. Navy's organization responsible for the procurement, storage, and deployment of all naval weapons before and during World War II.

- **The World War II Mk-14 Submarine Torpedo was deployed with four (4) major engineering flaws**
  - **"The war [WW-II] would have been foreshortened and many American lives saved had a reliable torpedo been available from the beginning … the cost to the United States war effort in lives, dollars, and time remain incalculable."**

— Vice Admiral Bernard M. Kauderer, USN(R), former Commander United States Submarine Forces

Bad Systems Engineering yields Bad Consequences

THE REACTIVE VS. PROACTIVE

Tolerable Consequence vs. Intolerable Consequence

- **According to Part 4-Highway Traffic Signals, Warrant 7, Crash Experience, it takes five (5) or more reported crashes within a 12-month period and exceeding one of the traffic volume requirements to get a traffic light at an intersection**
  (US DOT, FHA Manual on Uniform Traffic Control Devices – MUTCD)
  - **A reactive risk society; if its not broken don't fix it!**
  - **We "accept" the consequence that a minimum of five (5) reportable accidents will occur (Reactive to "small" threat)**
- **The World War II Mk-14 Submarine Torpedo was deployed with four (4) major engineering flaws**
  - **"The war [WW-II] would have been foreshortened and many American lives saved had a reliable torpedo been available from the beginning … the cost to the United States war effort in lives, dollars, and time remain incalculable."**
    Vice Admiral Bernard M. Kauderer, USN(R), former
    Commander United States Submarine Forces

Reactive with Tolerable Consequence: Proactive with Intolerable Consequence

- Are you building a system-of-interest that has “Intolerable Consequences” of failure
  - **Has the Customer/Owner (a.k.a., the Authorizing Official or AO) granted “Informed Consent” for the “Residual Risk” (or is it “Accepted Risk”)**
  - **Who, specifically, pays off the “technical debt” when the “Residual Risk” is realized**
    - For a traffic light, the 10 participants of the 5 crashes
    - For the Mk-14 Torpedo, it was “the cost to the United States [WW-II] war effort in lives, dollars, and time”

- Would you live in an area that experienced 35 rocket attacks, 99 terror attacks; that experienced 20 fatalities and 169 wounded?†
  - If you are Israeli, the answer is likely yes
  - If you are American, the answer is likely no
  - Are the Israeli's desensitized to their Risks?
- Is DoD desensitized to Cybersecurity Risks?

† *https://www.theyeshivaworld.com/news/israel-news/1443967/israel-in-2017-35-rocket-attacks-99-terror-attacks-and-20-fatalities-resulting-from-terror-attacks.html*

A PROCESS THE AT&T CO. USED IN THE 1930'S & 40'S THAT WAS DOCUMENTED BY ARTHUR D. HALL, III IN 1962 IN HIS SEMINAL BOOK, A METHODOLOGY FOR SYSTEMS ENGINEERING.

THE AFLC-WPAFB-DEC 69 CODIFIED THE EFFORT WITH MIL-STD-499 (USAF), SYSTEM ENGINEERING MANAGEMENT IN 19690717.

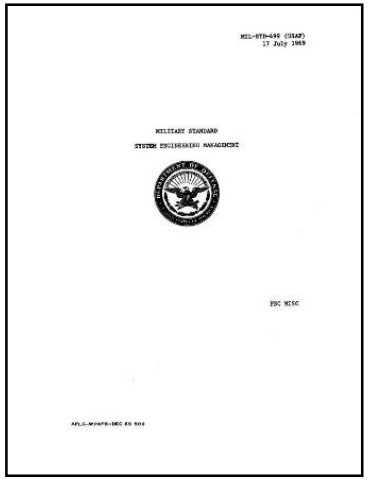
MARTIN MARIETTA CORPORATION CODIFIED THEIR "SYSTEMS ENGINEERING MANUAL" OF THE "NEW" TRI-SERVICE MIL-STD-499 IN 19691000

TODAY THEIR DESCENDENT ARE THE CONSENSUS STANDARD TRIPLETS OF ISO/IEC/IEEE 15288:2015(E) AND IEEE STD 15288.1™-2014 AND IEEE STD 15288.2™-2014

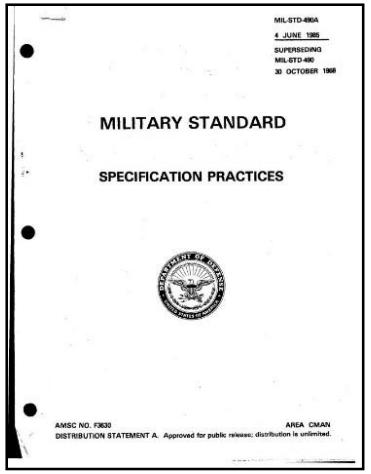
SYSTEMS ENGINEERING

MILITARY STANDARDS (ANCIENT HISTORY)

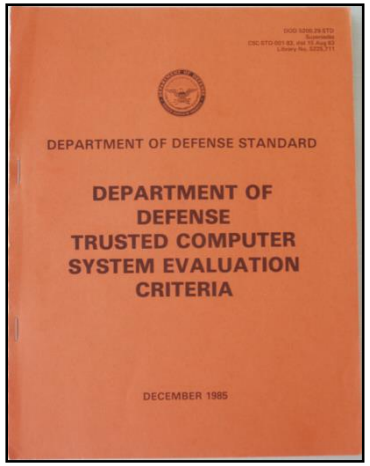
MIL-STD-499 19690717, System Engineering Management



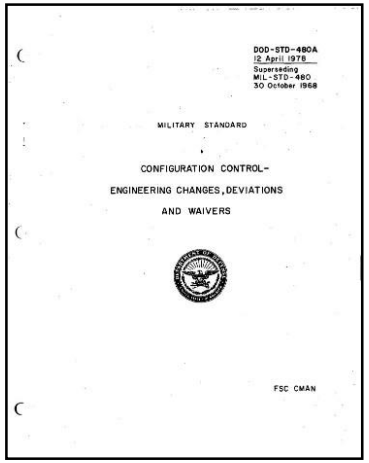
MIL-STD-490A 19850604, Specification Practices (superseding MIL-STD-490 19681030)



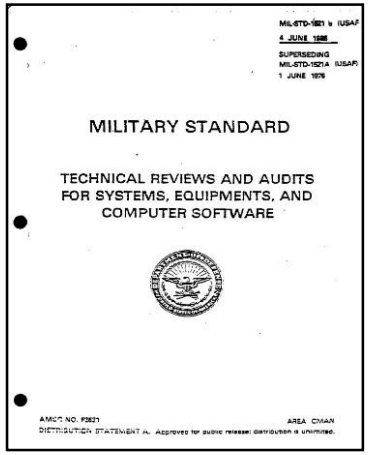
DoD Std 5200.28 Orange Book 19851226



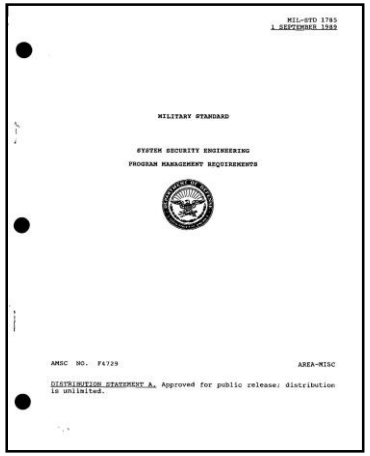
MIL-STD-480A 19780412, Configuration Control, Engineering Changes, Deviations and wavers (superseding MIL-STD-480 19681030)



MIL-STD-1521B 19850604, Technical Reviews and Audits for Systems, Equipment, and Computer Software (superseding MIL-STD-1521A 19760601)



MIL-STD-1785 System Security Engineering 19890901, Handbook as of 19950801 (Killed SSE)



NOTE: Mil-Std-1785 has been redesignated as a Handbook, and is to be used for guidance purposes only. For administrative expediency, the only physical change from Mil-Std-1785 is this cover page. However, this document Is no longer to be cited as a requirement. If cited as a requirement, Contractors may disregard the requirement of this document and Interpret its contents only as guidance.

MIL-HDBK-1785, DoD SYSTEM SECURITY ENGINEERING (SSE) OBITUARY OF 19950801

NOTE: Mil-Std-1785 has been redesignated as a Handbook, and is to be used for guidance purposes only. For administrative expediency, the only physical change from Mil-Std-1785 is this cover page. However, this document Is no longer to be cited as a requirement. If cited as a requirement, Contractors may disregard the requirement of this document and Interpret its contents only as guidance.

Contractors Only Implement Requirements that DoD Pays For

THE 15 PROGRAM PROTECTION COUNTERMEASURES

Table 2.2-1: CPI and Critical Components Countermeasure Summary (mandated) (sample)

	#	Protected Item (Inherited and Organic)	Countermeasures															
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
CPI	1	Algorithm QP	X	X	X	X	X	X	X		X					X	X	
	2	System Security Configuration											X			I		
	3	Encryption Hardware	X	X	X	X	X	X	X	X				X		X		
	4	IDS Policy Configuration	X	X	X	X	X	X	X	X						X		
	5	IDS Collected Data	X	X	X	X	X	X	I								I	
	6	KGV-136B	X	X	X	X			I		I				I			
Critical Components	7	iDirect M1D1T Hub-Line Card	X	X	X	X	X	X	X	X				X	X	X		
	8	Cisco Router IOS with Advance Security Option (ASO)	X	X	X	X	X	X								X		
	9																	
	10																	
	11																	
	12																	
	13																	

KEY *[Examples Included: UPDATE THIS LIST ACCORDING TO PROGRAM]*

	General CMs	Research and Technology Protection CMS	Trusted Systems Design CMs
Key **X =** Implemented **I =** Denotes protection already implemented if CPI is inherited	**1** Personnel Security **2** Physical Security **3** Operations Security **4** Industrial Security **5** Training **6** Information Security **7** Foreign Disclosure/Agreement	**8** Transportation Mgmt **9** Anti-Tamper **10** Dial-down Functionality	**11** IA/Network Security **12** Communication Security **13** Software Assurance **14** Supply Chain Risk Management **15** System Security Engineering (SSE) **16** Other

1. Personnel Security
2. Physical Security
3. Operational Security
4. Industrial Security
5. Training
6. Information Security
7. Foreign Disclosures/Agreements
8. Transportation Management
9. Anti-Tamper (AT)
10. Dial-down Functionality
11. Cybersecurity (former IA/Network Security)
12. Communications Security (COMSEC)
13. Software Assurance (SwA)
14. Supply Chain Risk Management (SCRM)
15. System Security Engineering (SSE)

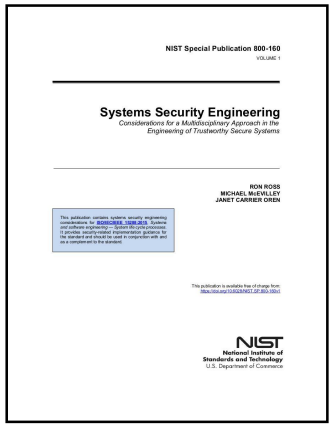
Government Program Protection Plan (PPP) Template of 20110718

TODAY'S SYSTEMS ENGINEERING DEFINED PROCESS; CONSENSUS AND INDUSTRY DEFINED STANDARDS

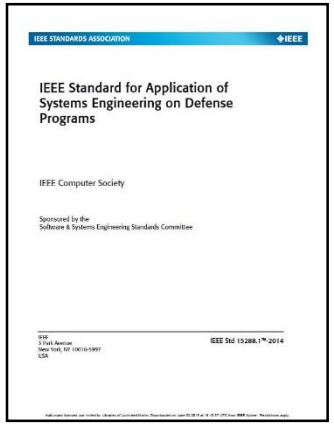
ISO-IEC-IEEE 15288 20150515 System life cycle processes

ISO-IEC-IEEE 15289 20150515 Content of life cycle information products (a.k.a., documents)

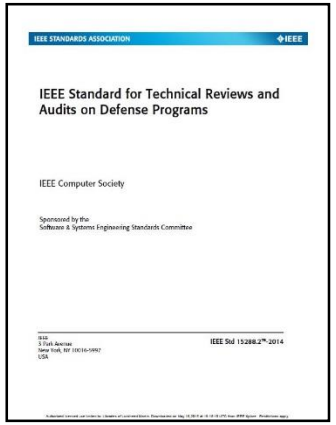
20161100 NIST SP 800-160v1 20180321 Systems Security Engineering



IEEE Std 15288.1™ 2014 Application of Systems Engineering on Defense Programs 20141210



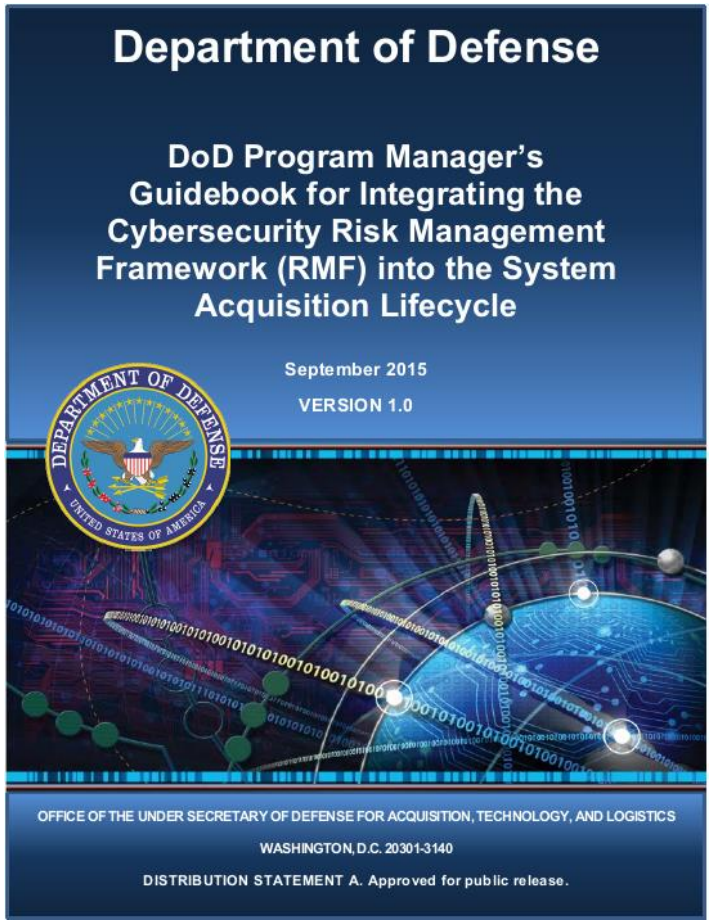
IEEE Std 15288.2™ 2014 Technical Reviews and Audits on Defense Programs 20141210



As Yogi Berra would say: Deja vu all over again.

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

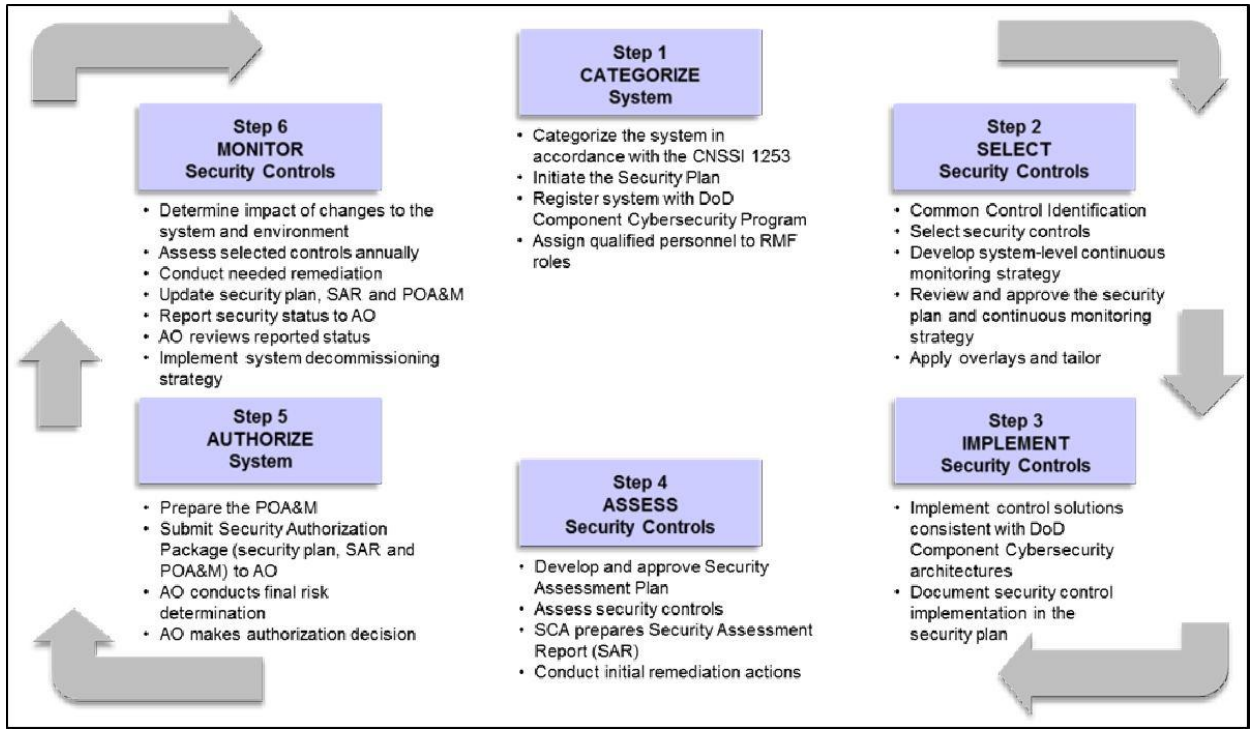
- Executive Summary
  - **"This guidebook emphasizes integrating cybersecurity activities into existing processes including requirements, SSE, program protection planning, trusted systems and networks analysis, developmental and operational test and evaluation, financial management and cost estimating, 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."



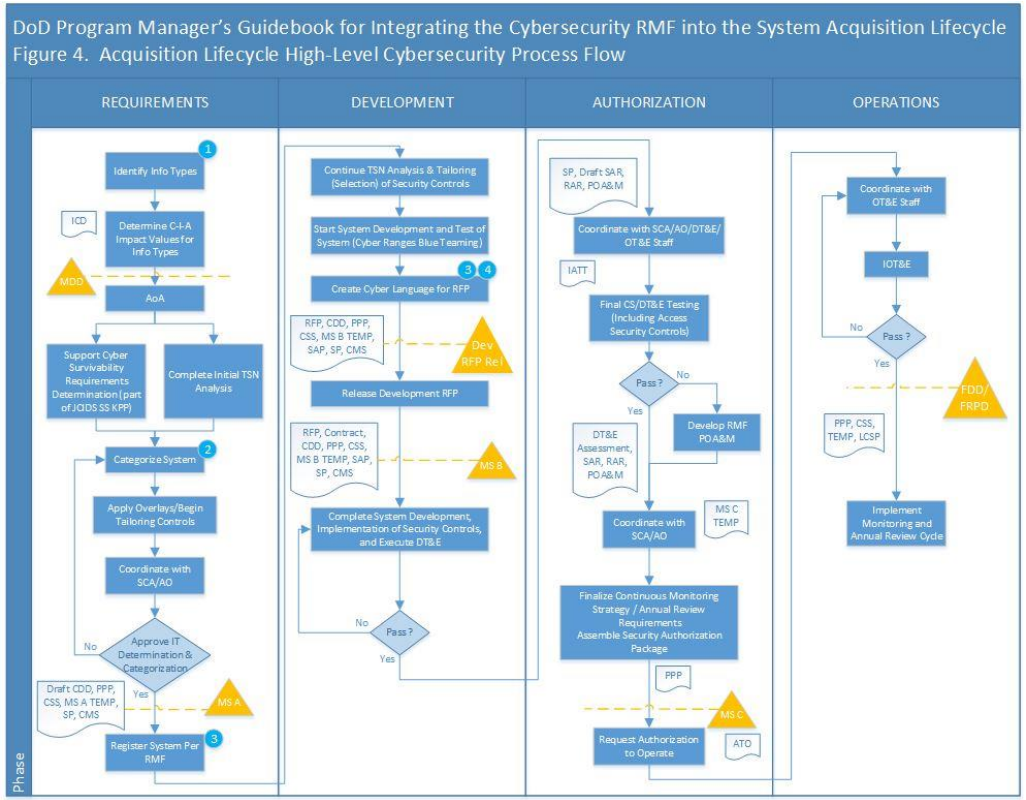
Eschew Suboptimization; Do Cybersecurity Early for an Optimum Total System Solution

DoD PM'S GUIDEBOOK FOR INTEGRATING THE CYBERSECURITY RMF INTO THE SYSTEM ACQUISITION LIFECYCLE

DoDI 8510.01 Enclosure 6, Figure 3, RMF for IS and PIT Systems

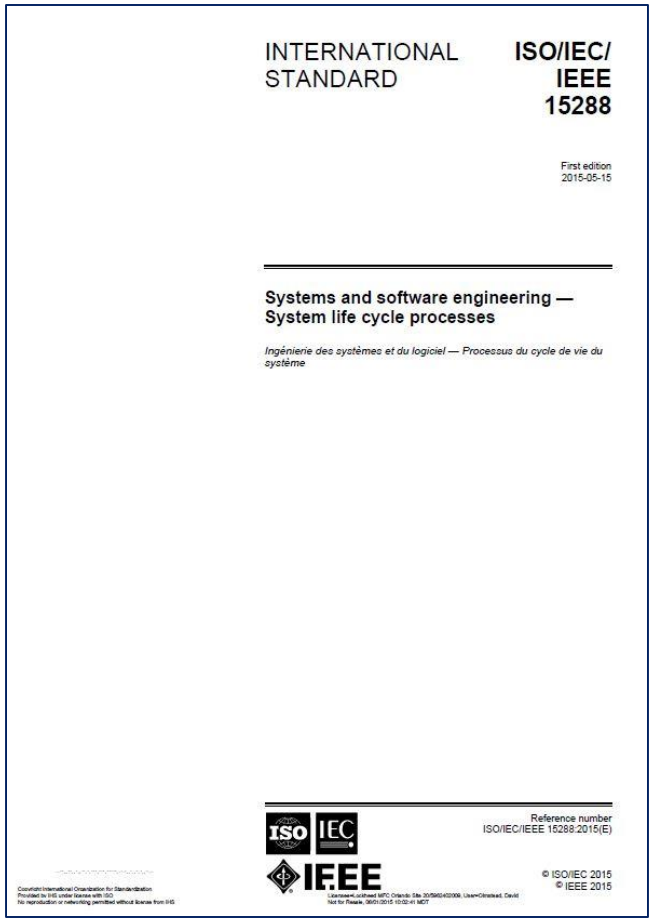


DoD PM's Guidebook Figure 4



Implementation Graphics Abound from Multiple Sources

ISO/IEC/IEEE 15288-2015(E)



INTERNATIONAL STANDARD

ISO/IEC/ IEEE 15288

First edition
2015-05-15

Systems and software engineering — System life cycle processes

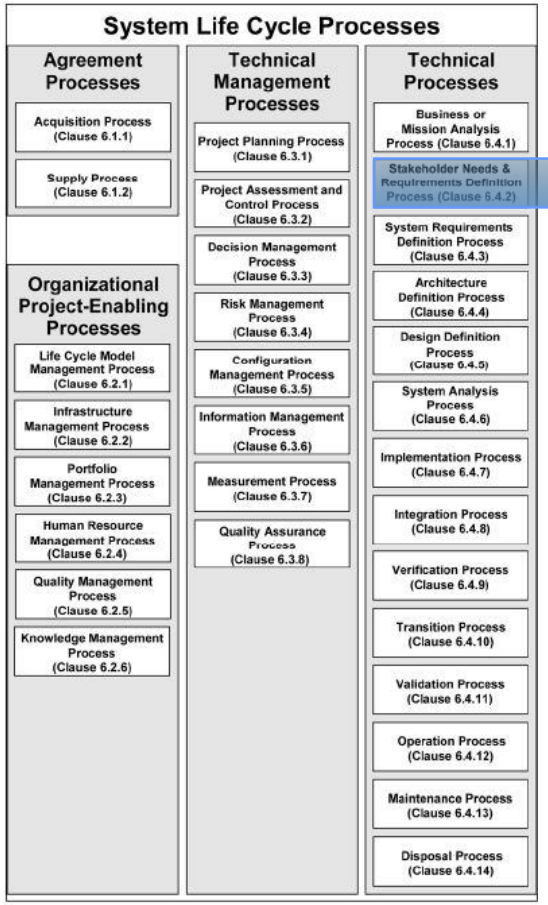
Ingénierie des systèmes et du logiciel — Processus du cycle de vie du système

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.”

The DoD Defined System Life Cycle Process Requirement

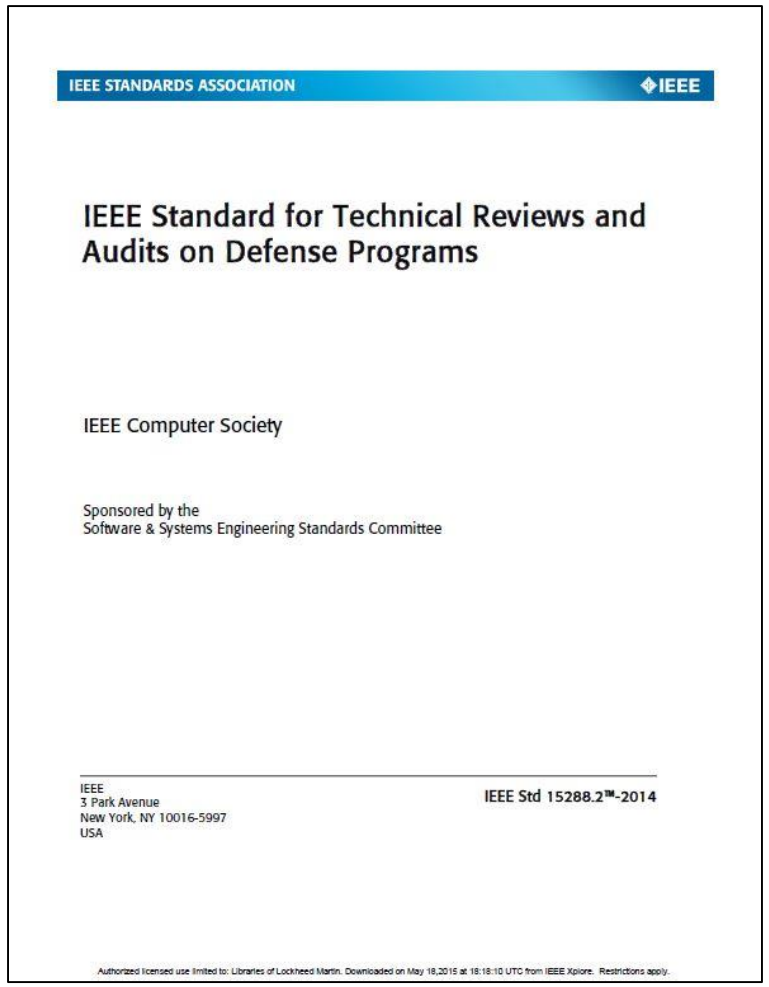
ISO/IEC/IEEE 15288-2015
THE REQUIREMENTS ENGINEER EARLY IN THE DEVELOPMENT



- **§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

IEEE STD 15288.2™-2014


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

- This standard addresses the needs of the defense community with respect to the incorporation, implementation, and execution of technical reviews and audits. IEEE Std 15288.1-2014, the standard that implements ISO/IEC/IEEE 15288 for application on defense programs, provides the defense-specific language and terminology to ensure the correct application of acquirer-supplier requirements for technical reviews and audits on a defense program, while this standard provides the implementation details to fulfill those requirements.

Defense Program Technical Reviews and Audits

IEEE STD 15288.2™-2014 TECHNICAL REVIEW TO BASELINES

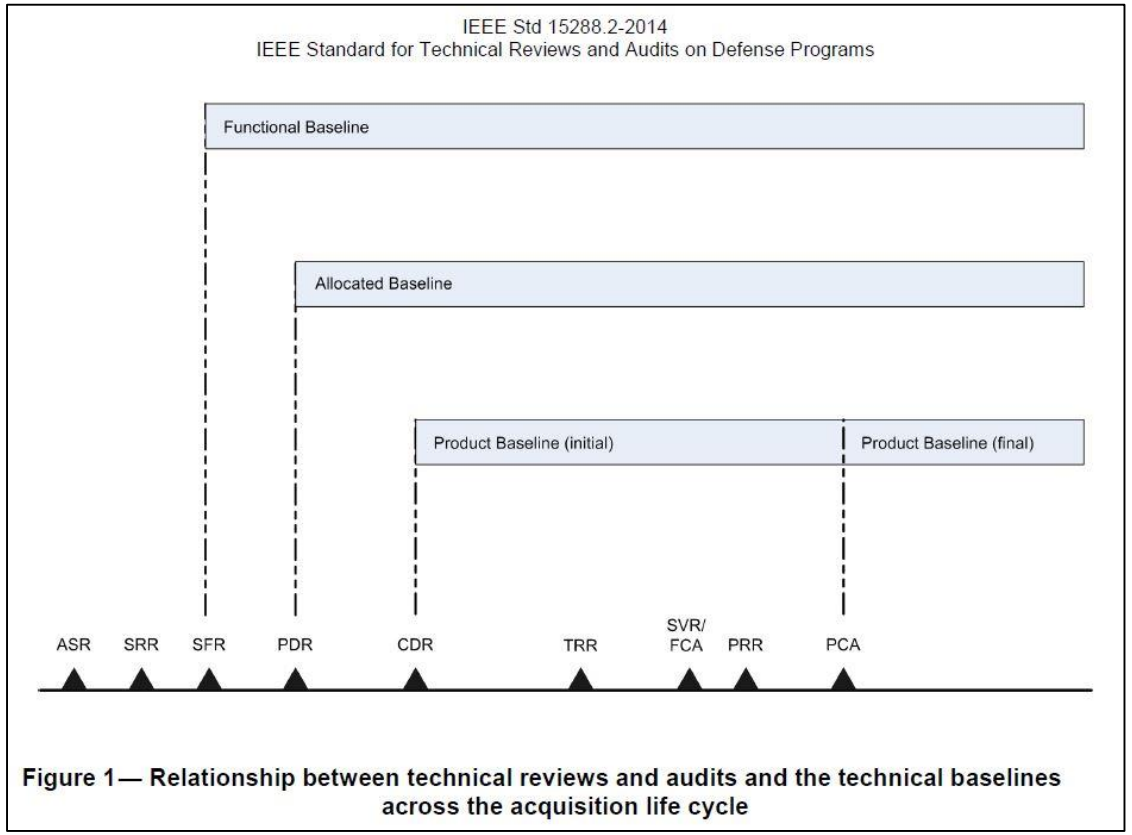
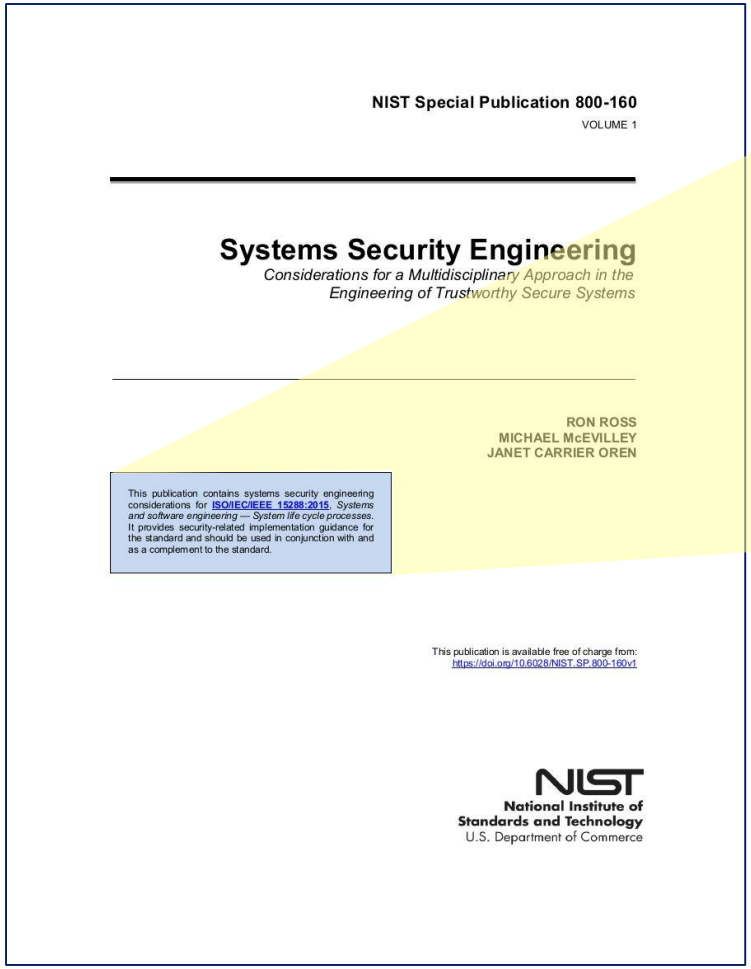


Figure 1— Relationship between technical reviews and audits and the technical baselines across the acquisition life cycle

- **The acquirer's SEP, and the supplier's Systems Engineering Management Plan (SEMP) where applicable, should define the technical reviews and audits selected for the program and their specific phasing across the program's life cycle. This standard provides application content for the following technical reviews and audits:**
  - **Alternative systems review (ASR)**
  - **System requirements review (SRR)**
  - **System functional review (SFR)**
  - **Preliminary design review (PDR)**
  - **Critical design review (CDR)**
  - **Test readiness review (TRR) [contained within the program's Test and Evaluation Master Plan (TEMP)]**
  - **Functional configuration audit (FCA)**
  - **System verification review (SVR)**
  - **Production readiness review (PRR)**
  - **Physical configuration audit (PCA)**

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

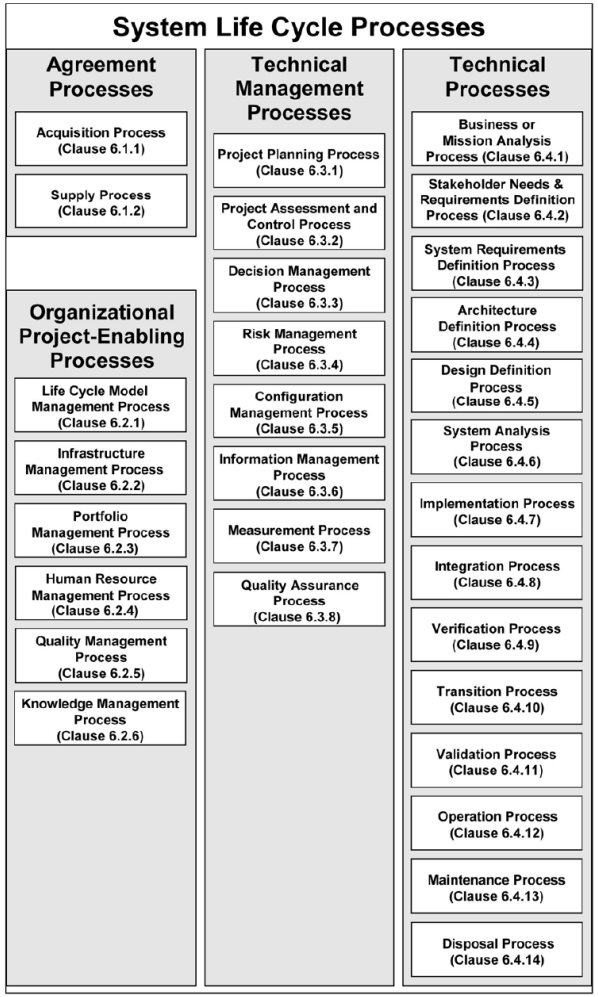
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

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



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

CORELATED ENCLAVE TO PIT SYSTEM / PIT WORK PRODUCTS

Enclave Work Products (Stove-Pipe)

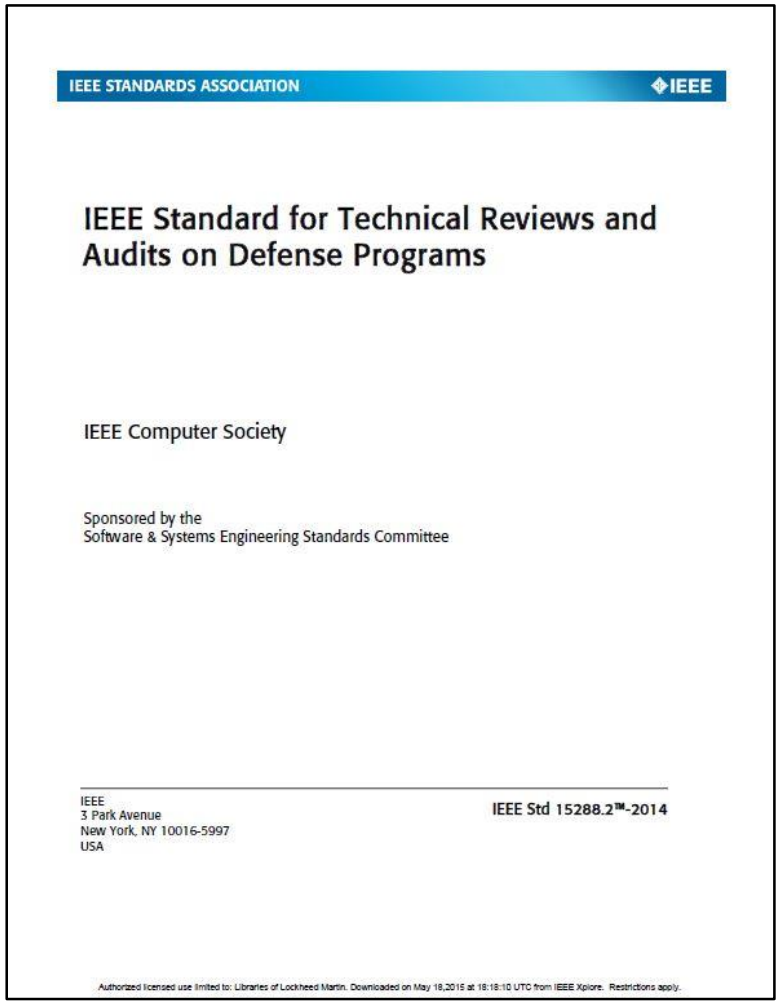
- **Cybersecurity Strategy**
- **System Security Plan (SSP) (RMS KS)**
  - **Ports, Protocols, & Services Management**
  - **DoD Security Control Set**
  - **System Authorization Boundary**
- **Continuous Monitoring Strategy (CMS) (NIST SP 800-137 ISCM)**
- **Security Assessment Plan (SAP)**
- **Security Assessment Report (SAR)**
- **Risk Assessment Report (RAR)**
- **Plan of Action and Milestones (POA&M)**

PIT System / PIT Work Products (Integrated)

- **PPP/PPIP at Appendix E (DoD CIO memo of 20151110 w/template)**
- **System Requirements Specification (SyRS), etc., flow-down Spec.**
  - **§2 Applicable Documents (Internal/External ICDs tied to §6.1 DoDAF SV-1, SV-3)**
  - **§3 Requirements (against HWCI/CSCI Critical Component from PPIP Appendix C) with System-of-Interest C-I-A & Overlays (from NIST SP 800-53r4 and associated CCIs)**
  - **§6.1 Intended Use (to include DoDAF OV-1 High-Level Operational Concept Graphic, DoDAF SV-1 Systems Interface Description, and SV-3 Systems-Systems Matrix)**
- **Cybersecurity Section of SEMP (Tier 1 and/or 2), SyRS §6.1 Intended Use (System-of-Interest Tier 3 Strategy) and PPIP**
- **TEMP Cybersecurity Section & SyRS (w/flow-down) §4 Verification**
- **SyRS (w/flow-down)§4 Verification Reports**
- **Pre MS-A & B Analysis Reports (Design Residual Risk) and Cybersecurity Section of DT&E/OT&E for Requirement Compliance**
  - **Note, the 15288/800-160 (§6.4.2.3e/§3.4.2 SN-5) Analyze Stakeholder Security Requirements Report "Defines" Design SySR Residual Risk for System-of-Interest**
- **Engineering Change Proposal (ECP) / Preplanned Product Improvement (P3I)**

PIT Acquisition Systems Engineering Includes Enclave "Stove-Pipe" Work Products

IEEE STD 15288.2™-2014


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

- §6.3 System requirements review (SRR) detailed criteria
- Table 5 – SRR technical review products acceptable criteria
  - **Product: System specification:**

m) System command, control, communication, computer, and intelligence (C4I) requirements are assessed and preliminary performance is allocated across segments and subsystems.
n) System security engineering (SSE), communications security (COMSEC), cybersecurity, and program protection (PP) antitamper security requirements are documented for each preliminary system conceptual architecture in accordance with DoD directives.
o) Preliminary cybersecurity requirements for both hardware and software are documented that address system data protection, availability, integrity, confidentiality, and authentication, and nonrepudiation and are consistent with the National Institute of Standards and Technology (NIST) risk management framework certification and accreditation requirements.
p) Cybersecurity requirements are mapped for each preliminary logical architecture.
q) Threat scenario assessments are completed, threat environments, categories of expected threats and their likelihood of occurrence are defined and correlated with preliminary system logical architectures, survivability and vulnerability KPPs are established for each assessed threat and correlated with the preliminary logical architectures.
hh) Requirements allocations and associated rationale from the source documents to the system specification have been documented.
ii) System specification is approved, including stakeholder concurrence, with sufficiently conservative requirements to allow for design trade space.
Etc.

Cybersecurity is "Built Into" Defense Program Technical Reviews and Audits

CYBERSECURITY IN DoD ACQUISITION OF DEVELOPMENTAL CONFIGURATION ITEMS (I.E., PIT MATERIEL PROCUREMENT)

- Recognize the need for Security within the System-of-Interest (i.e., PIT) at MDD
- Include Cybersecurity (and other Security, e.g., AT, SwA, SCRM) with all the other System-of-Interest Requirements (System Survivability KPP)
- For National Security Systems (NSS a.k.a., weapons, etc.) execute CNSSI 1253 Chapter 3
- Between Alternative System Review (ASR) and System Requirements Review (SRR) resolve Competing and Conflicting Requirements (Required Requirements Engineering)
  - **Publish System-of-Interest System Requirements Specification (SyRS)**
  - **The Cybersecurity Competing and Conflicting Requirements Analysis Report Defines the System-of-Interest (SoI) "Residual Risk" and requires AO/ISSM Approval**
    - Milestone B Entrance Criteria (RMF Step 2+ (Select), vice waiting to RMF Step 5 (Authorize))
    - The SoI "Residual Risk" report is analogous to an Enclave Risk Assessment Report (RAR)
      - P3I or ECP addresses SoI Non-compliance (POA&M addresses Enclave vulnerabilities)
  - **All SyRS Requirements will be "Compliant" and "Verified" (SyRS §4 Verification)**
- Follow the normal DoD Acquisition Process to obtain a Compliant SoI

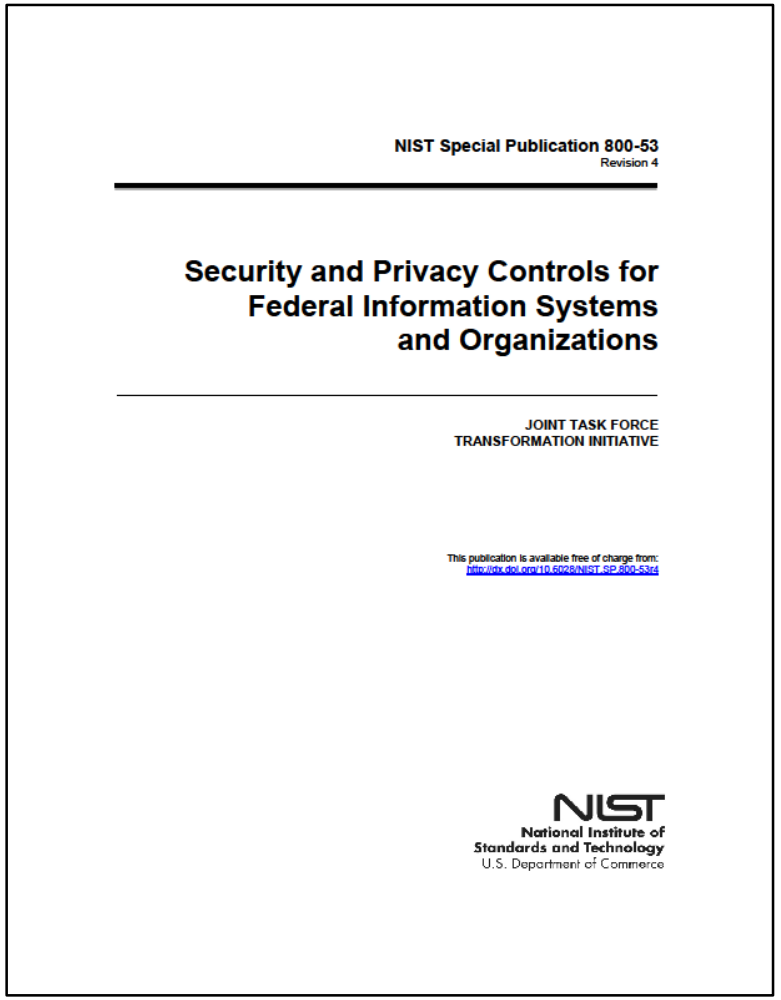
Built In Cybersecurity using Requirements Engineering is the only Affordable Solution

HAVING IDENTIFIED THE INFRASTRUCTURE NEEDS FOR PRODUCT DEVELOPMENT THE REMAINDER OF THE PRESENTATION WILL:

FOCUS ON THE PRODUCT

SOURCE DOCUMENTS

NIST SP 800-53r4 NIST SP 800-53Ar4 CNSSI 1253



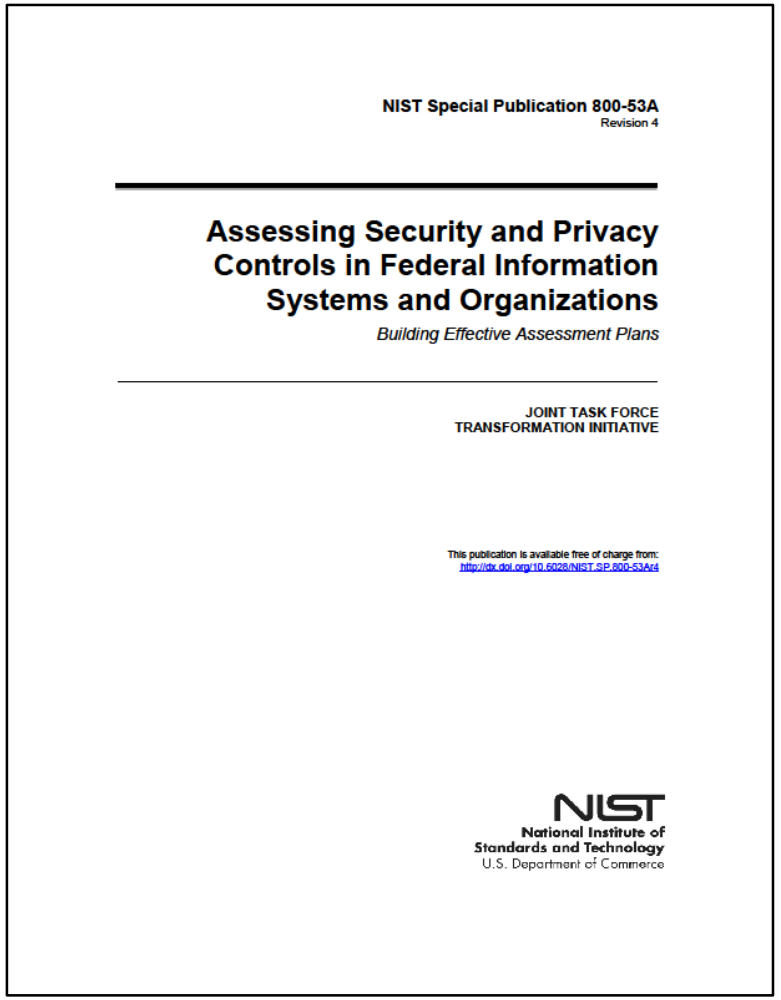
NIST Special Publication 800-53
Revision 4

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 Special Publication 800-53A
Revision 4

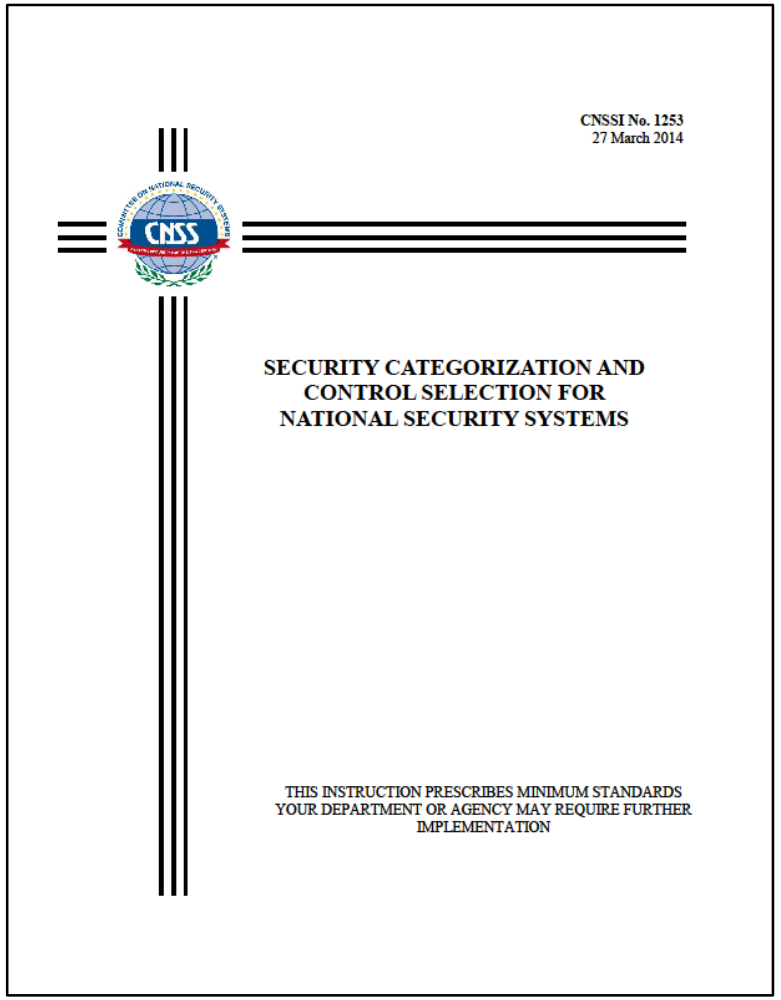
Assessing Security and Privacy Controls in Federal Information Systems and Organizations

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



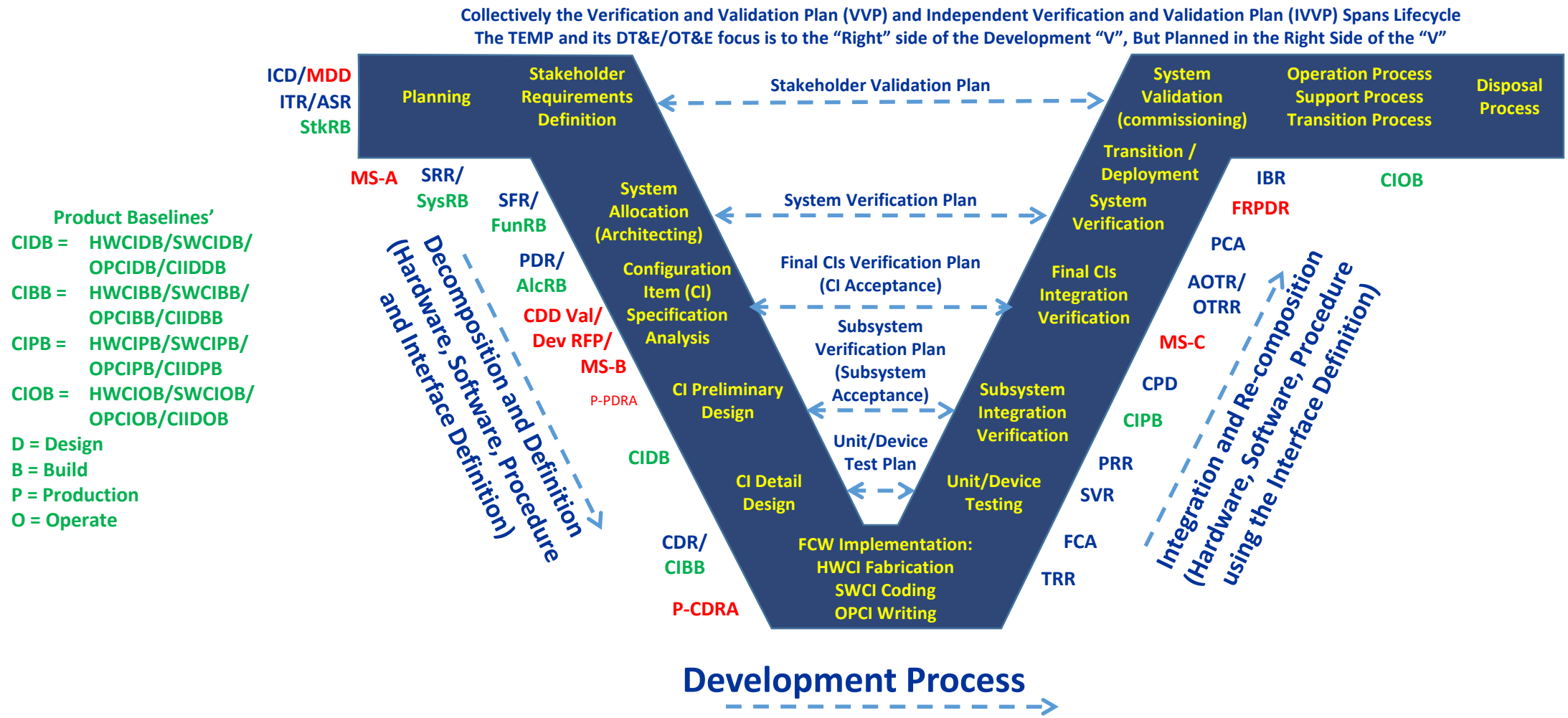
CNSSI No. 1253
27 March 2014

CNSS

SECURITY CATEGORIZATION AND CONTROL SELECTION FOR NATIONAL SECURITY SYSTEMS

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

DoD AT&L PRODUCT LIFE CYCLE PROCESS



Nothing New; The original "V-Chart" was first presented at NCOSE (now INCOSE) in 1991

BASELINE LANGUAGE PROGRESSION CYBERSECURITY'S REQUIREMENT PROGRESS

Your Starting Point in the Process i.e., You Are Here

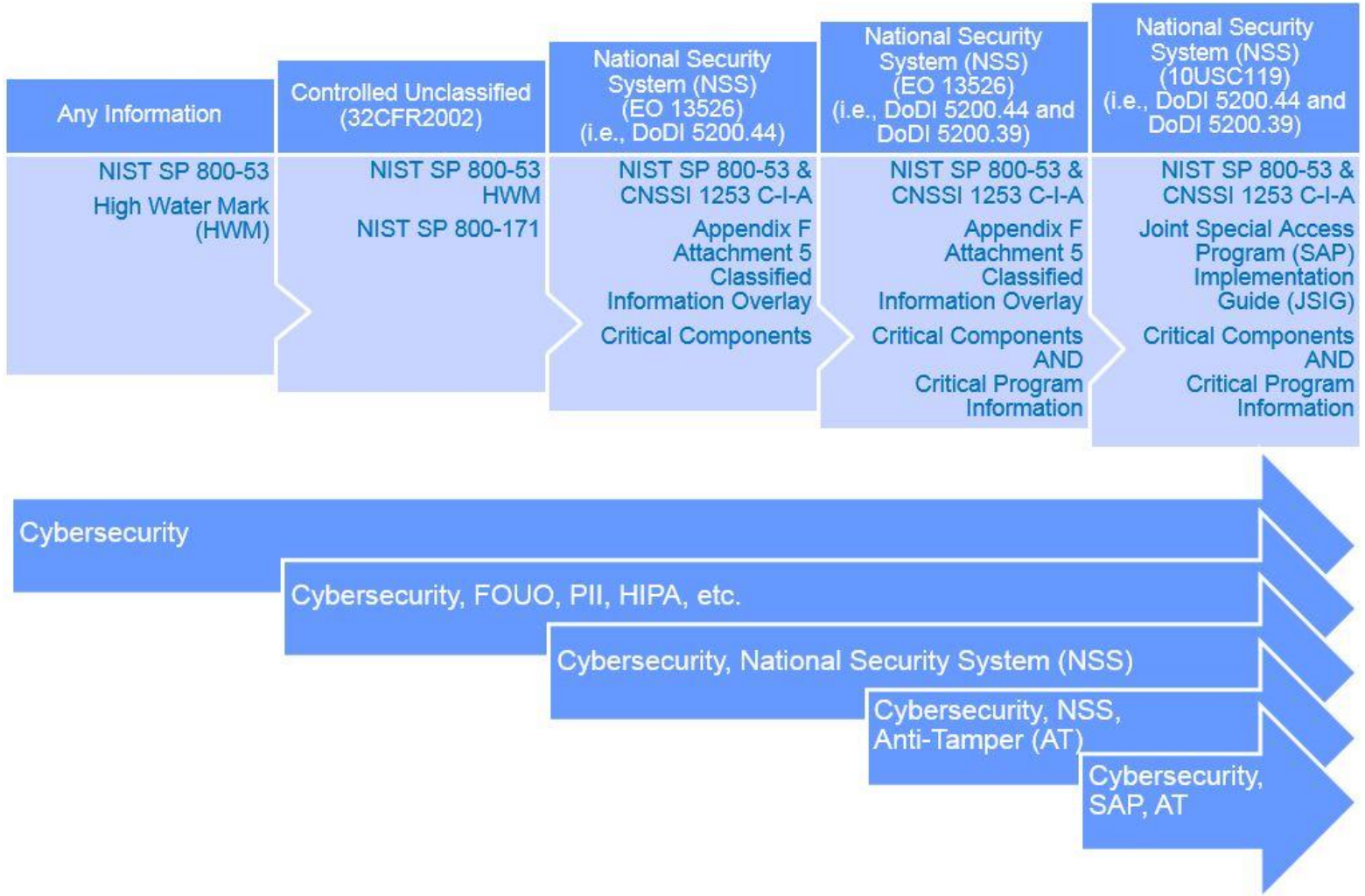
You get your Stakeholder Requirements from NIST SP 800-53r4 and their Verification from NIST SP 800-53Ar4 via CNSSI 1253

Stakeholder Requirements Baseline	Customer Speak	System Documents (Requirements Configuration)	Stakeholder Competing and Conflicting Requirements
System Requirements Specification	Agnostic System Speak	System Documents (Requirements Configuration)	Stakeholder Competing and Conflicting Requirements
Functional Requirements Baseline	Agnostic System Speak	System Documents (Requirements Configuration)	De-conflicted Inter- Intra-Stakeholder Requirements
Allocated Requirements Baseline	Domain System Speak	System Documents (Requirements Configuration)	HWCIs, SWCIs, OPCIs, CIIDs Requirement Specifications
F/C/W Design Baseline	Domain Design Speak	Domain Documents (Domain Configuration)	HWF Design, SWC Design OPW Design, IDF/C/W Design
Product Baseline	Domain Product Speak	Domain Documents (Product Configuration)	Fabricated, Coded and Written Configuration Items

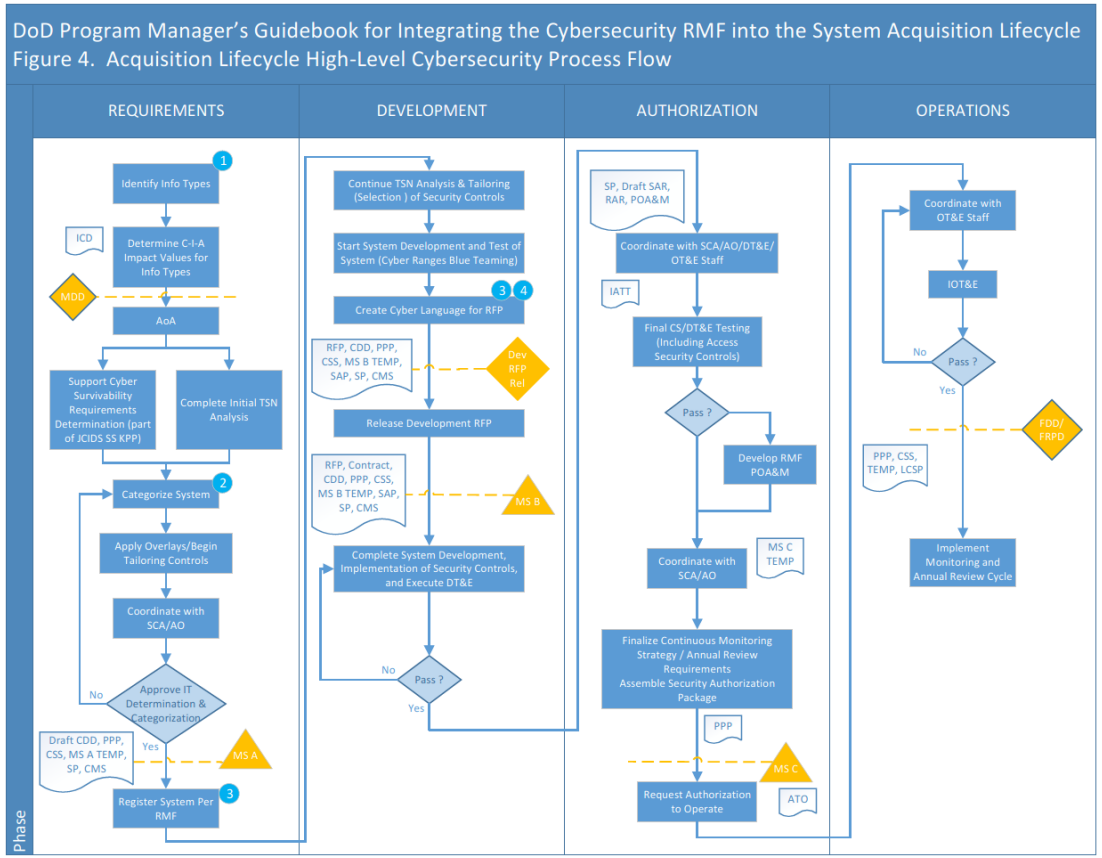
If you don't include security from the beginning, you have "Sub-optimized" the system and created an "Un-Affordable" solution

Cybersecurity's Position Along the Life Cycle Progression

THE PROGRESSION OF CYBERSECURITY IN DoD



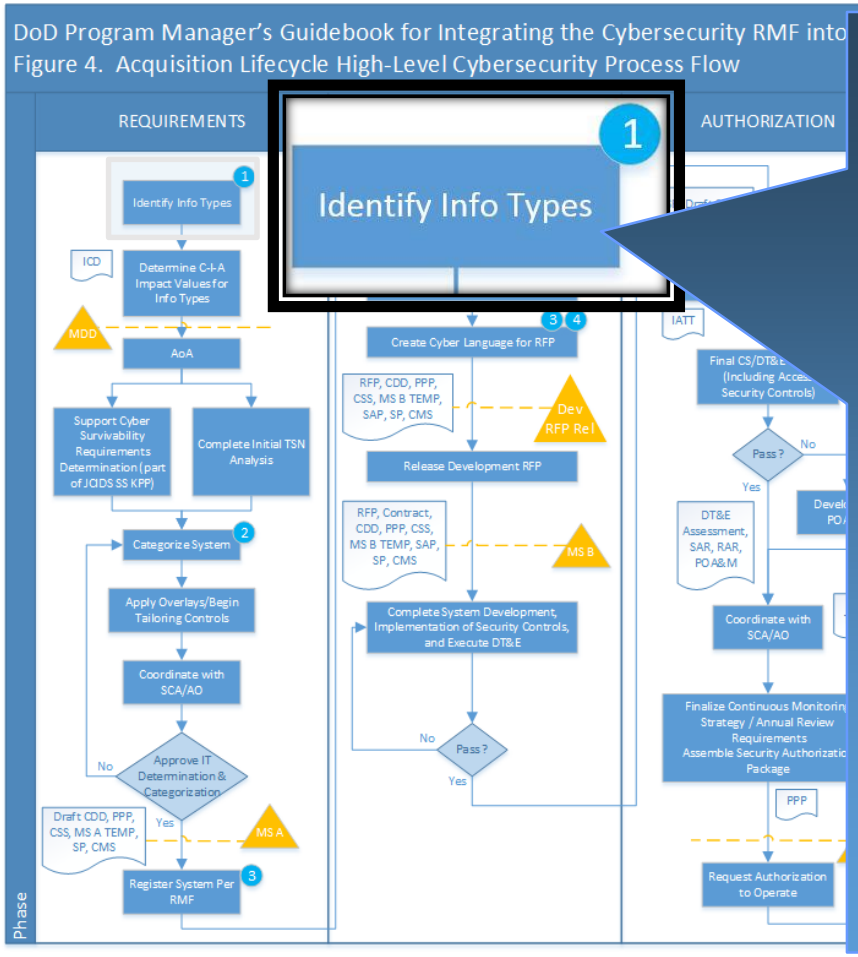
DoD PM'S GUIDEBOOK, CYBERSECURITY PROCESS FLOW



- If you do the "Requirements" Acquisition Lifecycle High-Level Cybersecurity Process Flow
  - **Good Systems Engineering System-of-Interest Work per ISO/IEC/IEEE 15288:2015(E) will yield "Development", "Authorization", and "Operations" Process Flow as a Natural Outcome**

Start With Good Requirements Engineering to Achieve Optimal Total System Solution

INTEGRATING RMF INTO DoD ACQUISITION: CLASSIC DoD INFORMATION TYPES

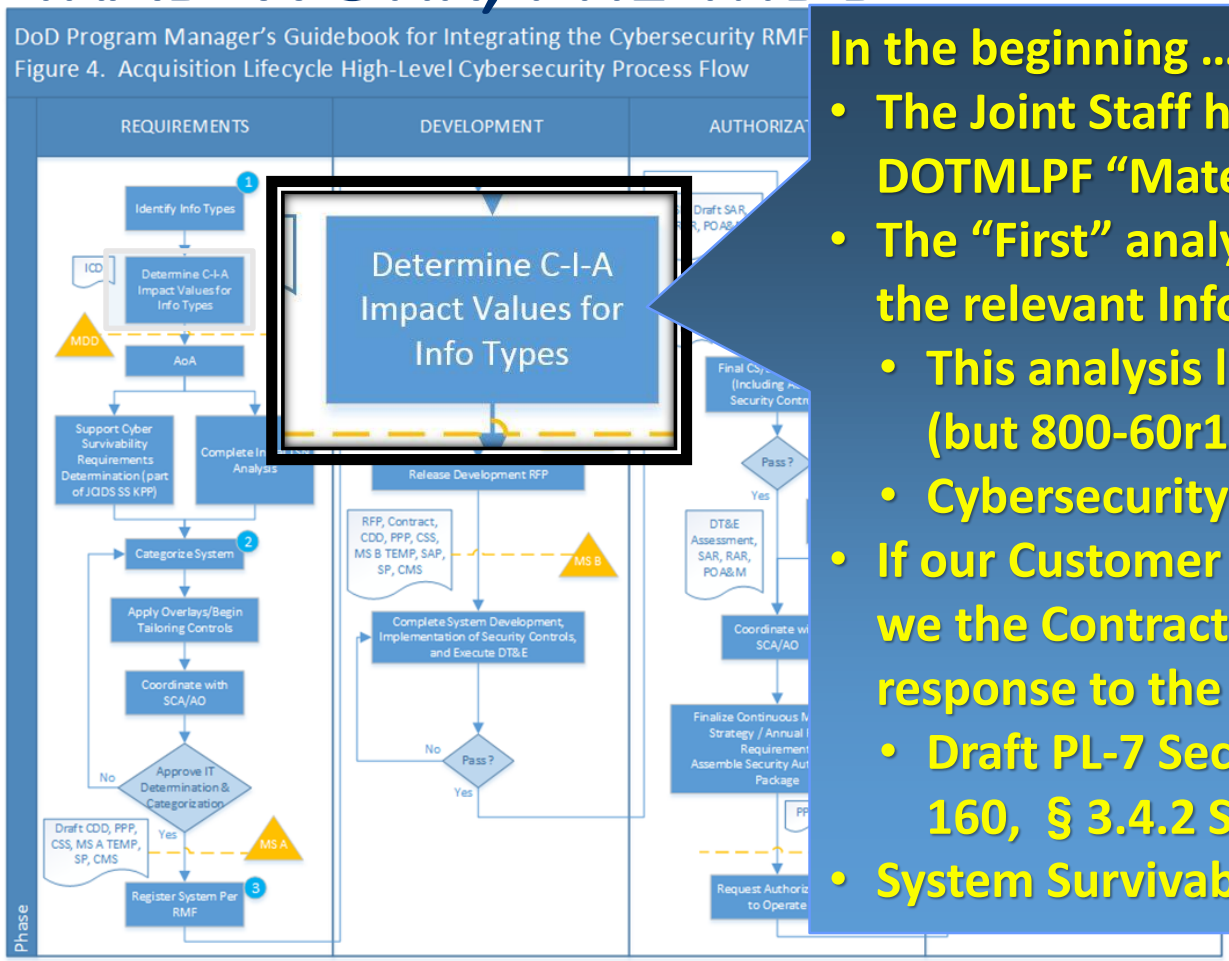


Identify Information Types (in DoD PIT System or PIT)

- **Cleared For Public Release**
- **Federal Contract Information (48CFR52.204)**
- **Controlled Unclassified Information (CUI) (32CFR2002) and NIST SP 800-171 (e.g., "Covered Defense Information", Controlled Technical Information", as defined in DFARS 252.204-7012 etc.)**
- **Classified Information (e.g., EO 12526 or SAP/Waived SAP [10USC119])**
- **CNSSI 1253, Appendix F, Attachment 6, Privacy Overlay 20150420**
- **Etc.**

The Same Process but Different "Information Types" as NIST SP 800-60

INTEGRATING RMF INTO DoD ACQUISITION: IRAD WORK, PRE-MDD



In the beginning … Above the MDD line

- **The Joint Staff has a CONOPS (see CJCSI 3010.02D) that yields a DOTMLPF "Materiel" Need as an ICD**
- **The "First" analysis of the ICD and "Materiel" Need to determine the relevant Information Types and their associated C-I-A**
  - **This analysis looks something like NIST SP 800-60r1 Volumes I & II (but 800-60r1 is N/A for NSS)**
  - **Cybersecurity Supporting Joint Concept**
- **If our Customer Stakeholder does not give us this information then we the Contractor must "Synthesize" as a Proposal Assumption in response to the RFP**
  - **Draft PL-7 Security Concept of Operation (and see NIST SP 800-160, § 3.4.2 SN-3 & 15288 § 6.4.2.3.c)**
- **System Survivability Key Performance Parameter**

There are 10 Cyber Survivability Attributes (CSAs) under the KPP

SECURITY CATEGORIZATION – IMPACT VALUE FOR INFORMATION TYPES, NSS

Confidentiality (C)

Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information
[44 U.S.C. 3552]

A loss of confidentiality is the unauthorized disclosure of information.

Integrity (I)

Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity
[44 U.S.C. 3552]

A loss of integrity is the unauthorized modification or destruction of information.

Availability (A)

Ensuring timely and reliable access to and use of information
[44 U.S.C. 3552]

A loss of availability is the disruption of access to or use of information or an information system.

Low (L)

The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.
[FIPS PUB 199 & CNSSI 1253]

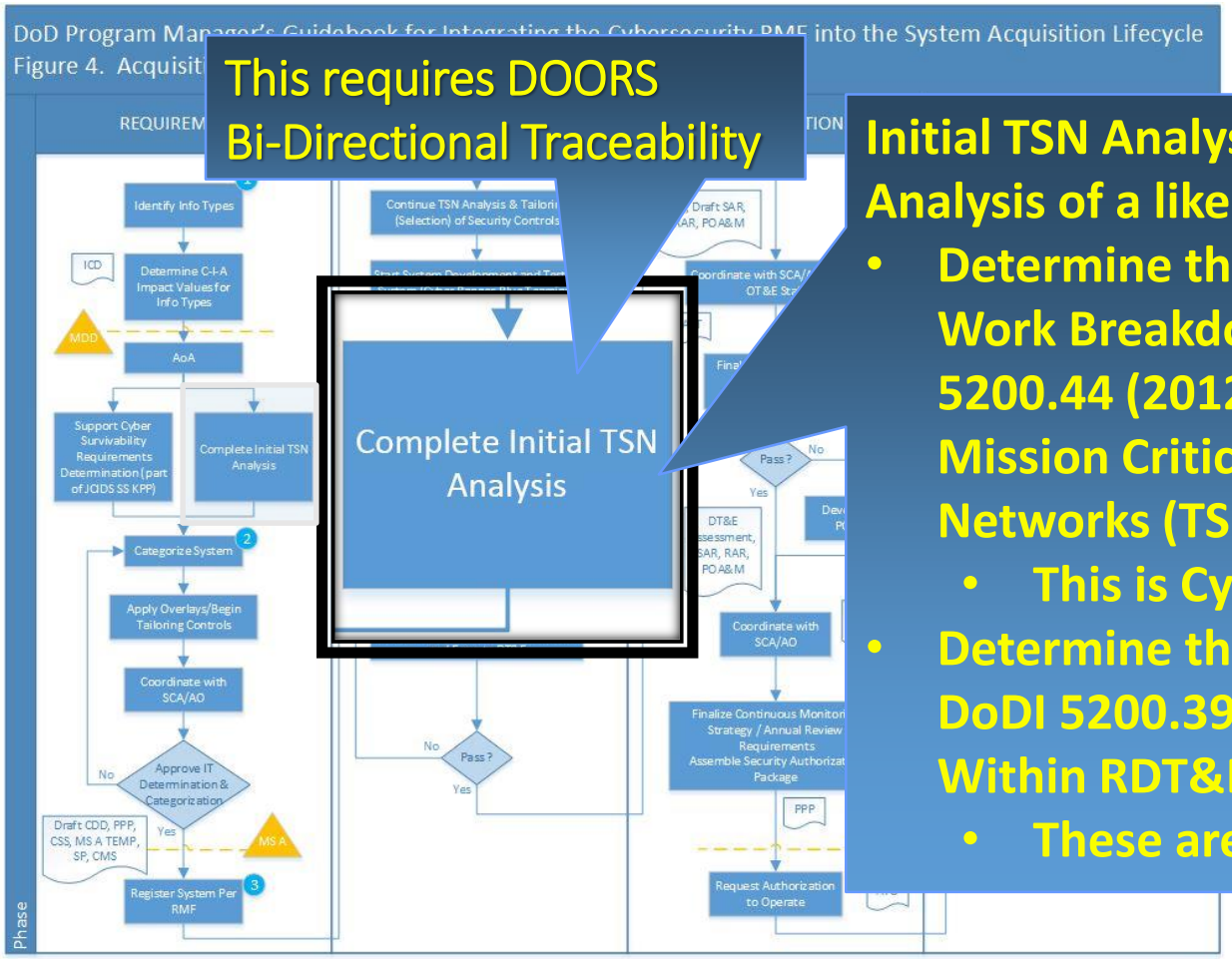
Moderate (M)

The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals, ***exceeding mission expectations***.
[FIPS PUB 199 & CNSSI 1253]

High (H)

The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals, ***exceeding mission expectations***.
[FIPS PUB 199 & CNSSI 1253]

INTEGRATING RMF INTO DoD ACQUISITION: IRAD WORK, PRE-MILESTONE A (MS A)

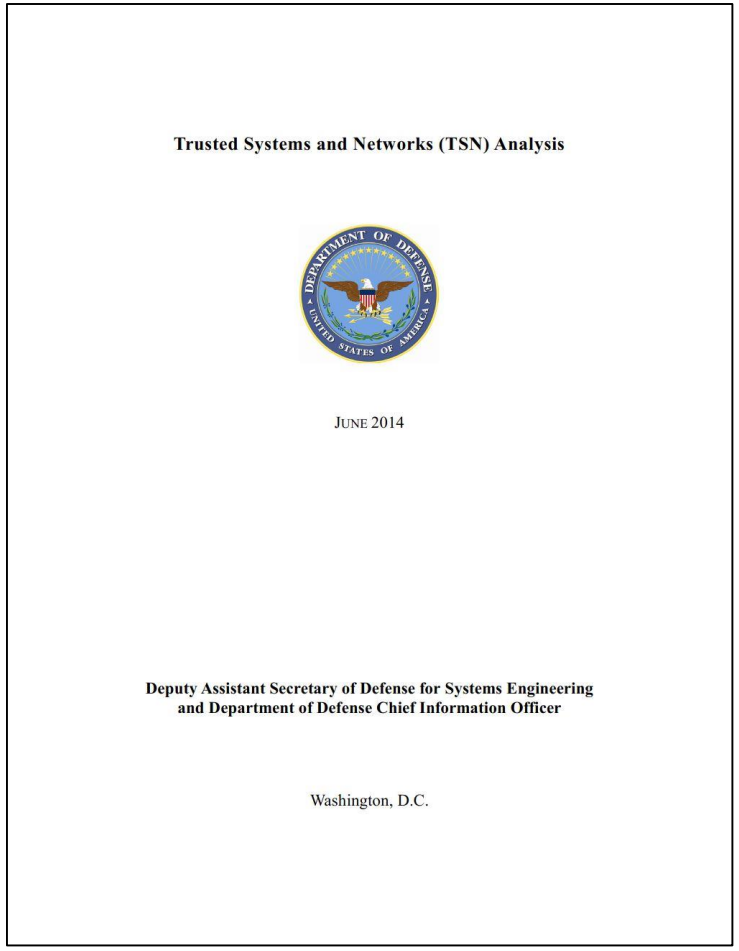


Initial TSN Analysis (i.e., this is the two [2] "Criticality" Analysis of a likely "Materiel" system-of-interest)

- **Determine the "Critical Components" (to a MIL-STD-881C Work Breakdown Structure level of detail) based on DoDI 5200.44 (20121105 w/Ch1 20160825) Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)**
  - **This is Cybersecurity Stuff**
- **Determine the "Critical Program Information" based on DoDI 5200.39 (20150528), CPI Identification and Protection Within RDT&E**
  - **These are Anti-Tamper Candidates**

We "Synthesize" (too) based on our Previous Assumptions

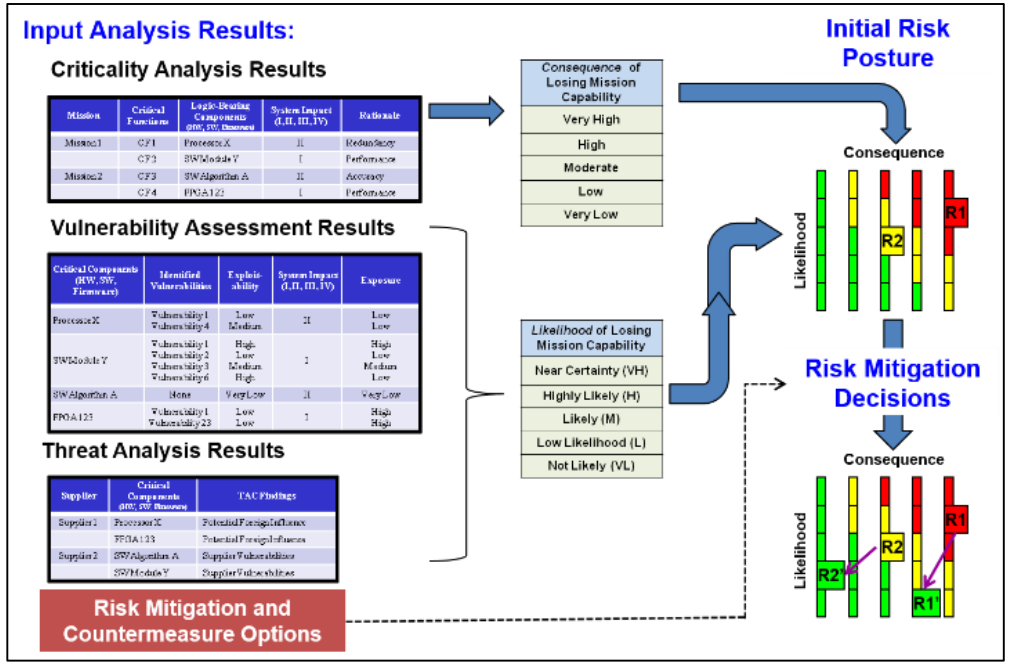
OSD SYSTEMS ENGINEER/DoD CIO TSN ANALYSIS


Trusted Systems and Networks (TSN) Analysis

JUNE 2014

Deputy Assistant Secretary of Defense for Systems Engineering
and Department of Defense Chief Information Officer

Washington, D.C.

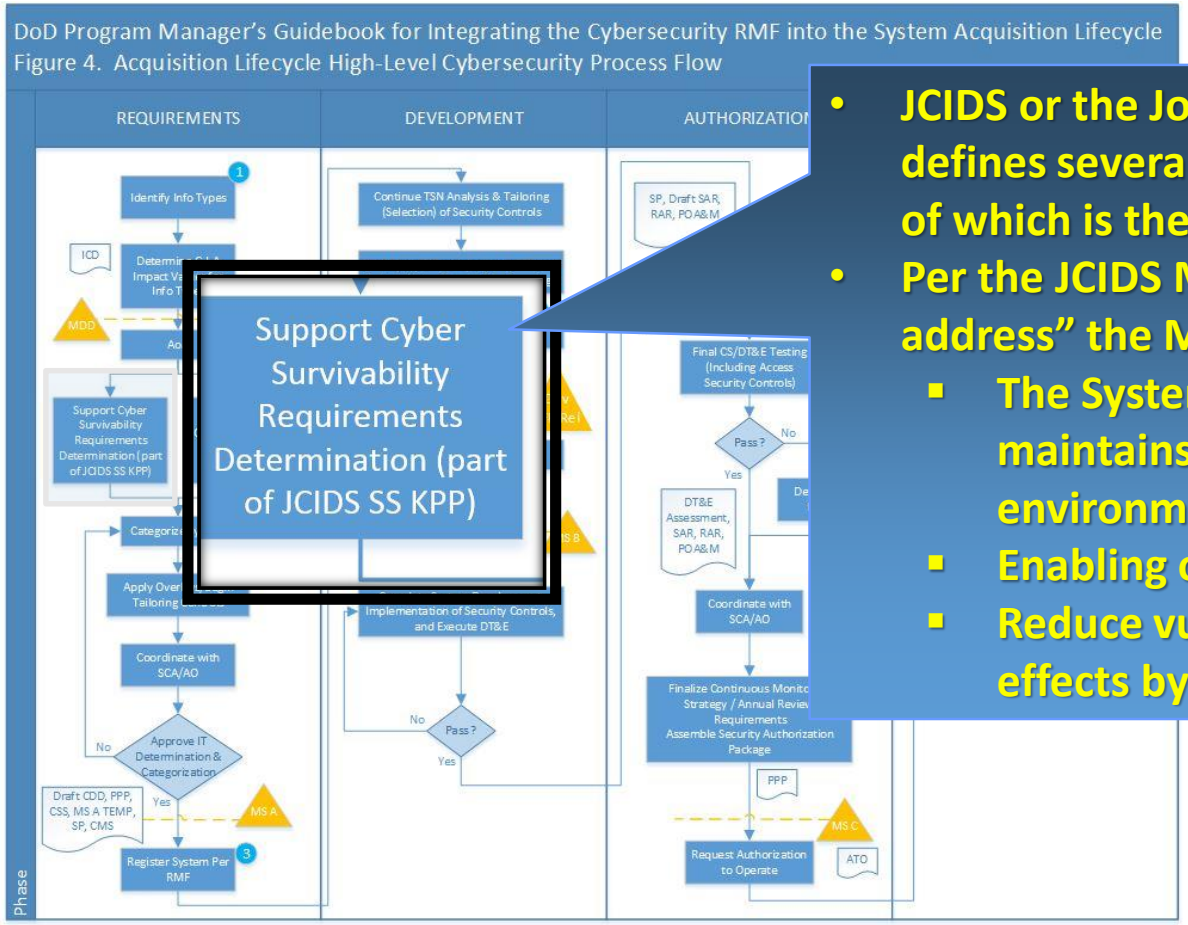


This document is intended as an extension to guidance provided in the Defense Acquisition Guidebook (DAG) Chapter 9 (former Ch-13), Program Protection. This document provides further details for Trusted Systems and Networks (TSN) analysis processes, methods, and tools. It elaborates on each of the major iterative processes necessary to accomplish the TSN analysis objectives.

- This Risk Analysis will occur at each SETR (i.e., SRR, SFR, PDR, CDR, & PRR) as defined in IEEE Std 15288.2™-2014 IEEE Standard for Technical Reviews and Audits on Defense Programs

This is an Iterative and Recursive Process

SYSTEM SURVIVABILITY (SS) KEY PERFORMANCE PARAMETER – JCIDS MANDATORY KPP

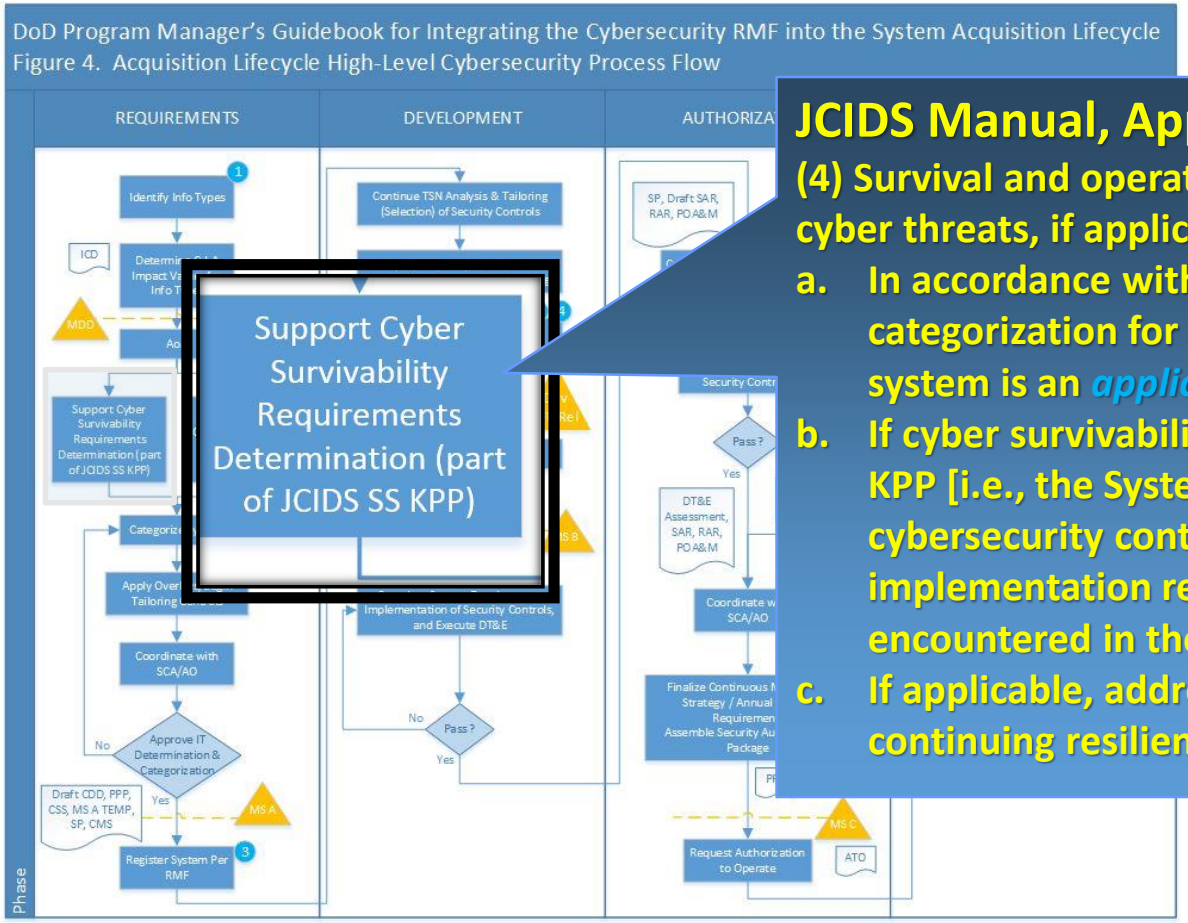


Support Cyber Survivability Requirements Determination (part of JCIDS SS KPP)

- JCIDS or the Joint Capabilities Integration & Development System defines several "Mandatory" Key Performance Parameters (KPPs), one of which is the System Survivability KPP
- Per the JCIDS Manual, "Sponsors [i.e., those that develop things] shall address" the Mandatory KPPs
  - The System Survivability (SS) KPP is intended to ensure the system maintains its critical capabilities under applicable threat environments …
  - Enabling operation in degraded … cyber environments
  - Reduce vulnerability if hit by non-kinetic fires, including cyber effects by means of "Durability" and "added protection"

System Survivability KPP – Cyber Survivability Attributes (CSAs)

SYSTEM SURVIVABILITY (SS) KEY PERFORMANCE PARAMETER – JCIDS MANDATORY KPP (CONTINUED)



Support Cyber Survivability Requirements Determination (part of JCIDS SS KPP)

JCIDS Manual, Appendix C, Enclosure D

(4) Survival and operation in a cyber-contested environment or after exposure to cyber threats, if applicable to the operational context:

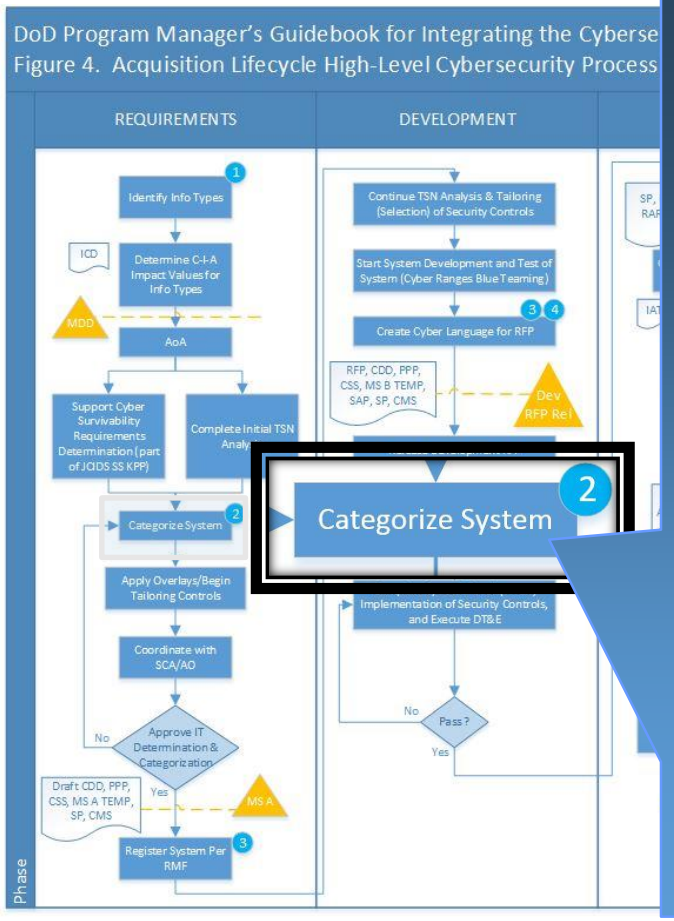
a. In accordance with [DoDI 8500.01], state the system's cybersecurity categorization for availability, integrity, and confidentiality and whether the system is an *applicable system* [see below] in accordance with [DoDI 5200.44].

b. If cyber survivability is required, include appropriate cyber attributes in the SS KPP [i.e., the System Survivability Mandatory KPP] based on applicable cybersecurity controls as directed by [DoDI 8500.01] and strength of implementation required to protect against cyber threats likely to be encountered in the operational environment.

c. If applicable, address operational and maintenance issues related to ensuring continuing resilience against cyber threats.

System Survivability KPP – Cyber Survivability Attributes (CSAs)

INTEGRATING RMF INTO DoD ACQUISITION: IRAD WORK, PRE-MILESTONE A (MS A)



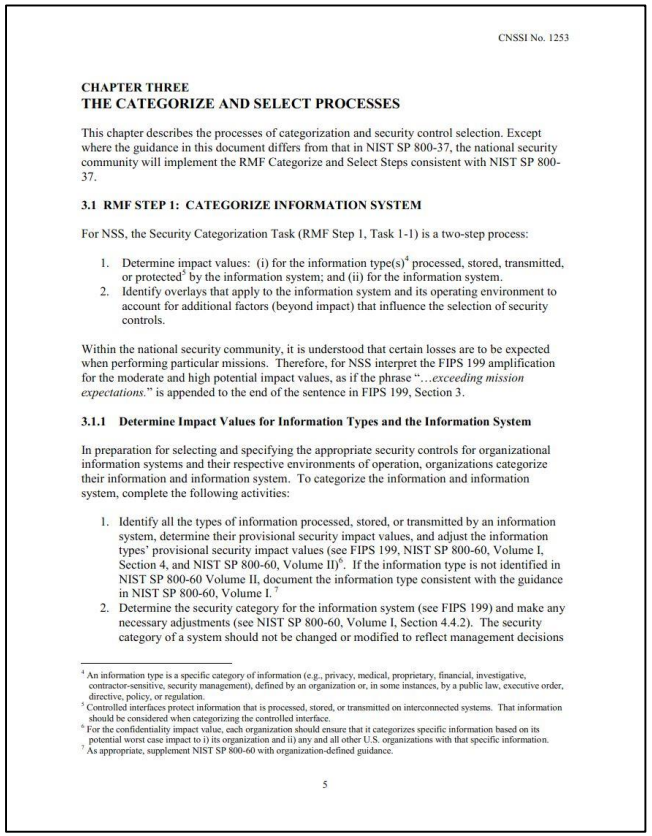
Recognize Correct Answer When Told (known method)

- **Follow "The Categorize and Selection Process" from CNSSI 1253, Chapter 3**
- **Verify that you are a FISMA 2014 NSS using NIST SP 800-59 Checklist (still holds from FISMA 2002)**
- **Select (90% of the DOORS work is done) appropriate DOORS Specifications:**
  - **NIST SP 800-53**
  - **NIST SP 800-53A**
  - **CNSSI 1253 Appendix F "Attachments"**
  - **NIST SP 800-161 (SCRM)**
  - **NIST SP 800-171 (Controlled Unclassified)**
  - **JSIG**
  - **NIST SP 800-160 (SSE)?**
- **Leverage the Existing Standard Answers**
  - **Personnel Security / Training / Configuration Management, etc.**

We "Synthesize" (again) based on our Previous Assumptions

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

Page 5



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.

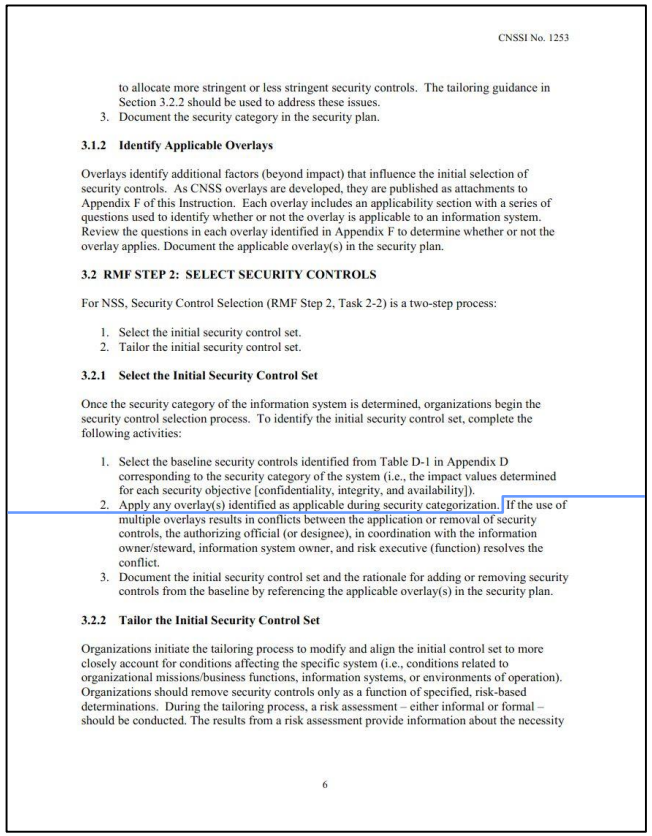
3.1.1 Determine Impact Values for Information Types and the Information System

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.

Page 6



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:

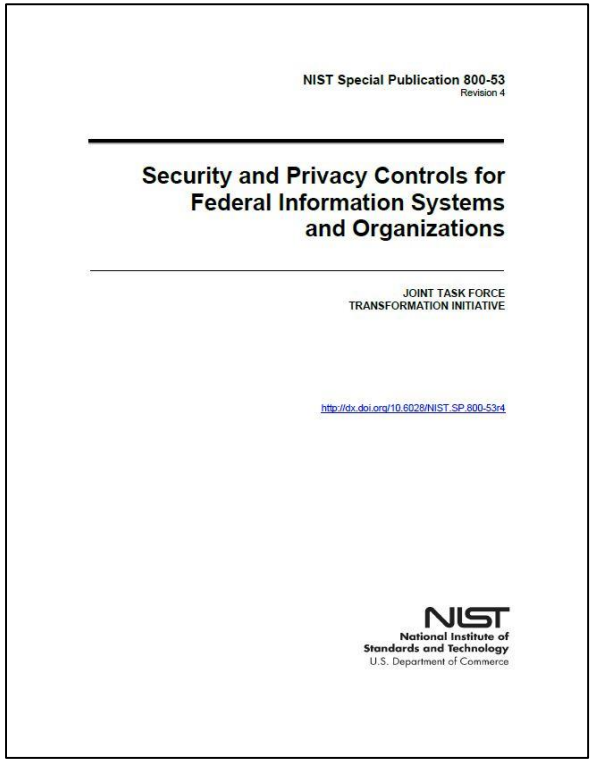
1. Select the baseline security controls identified from Table D-1 in Appendix D corresponding to the security category of the system (i.e., the impact values determined for each security objective [confidentiality, integrity, and availability]).
2. Apply any overlay(s) identified as applicable during 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

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

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

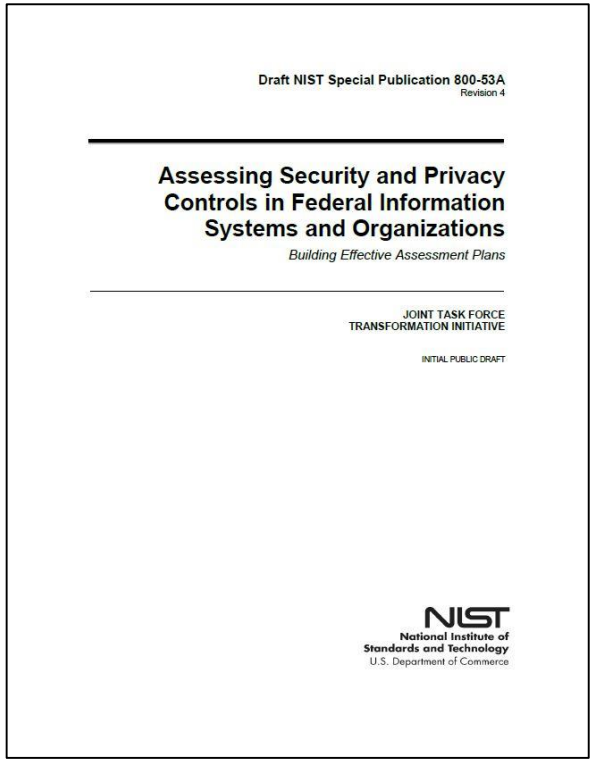
Security and Privacy Controls for Federal Information Systems and Organizations

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

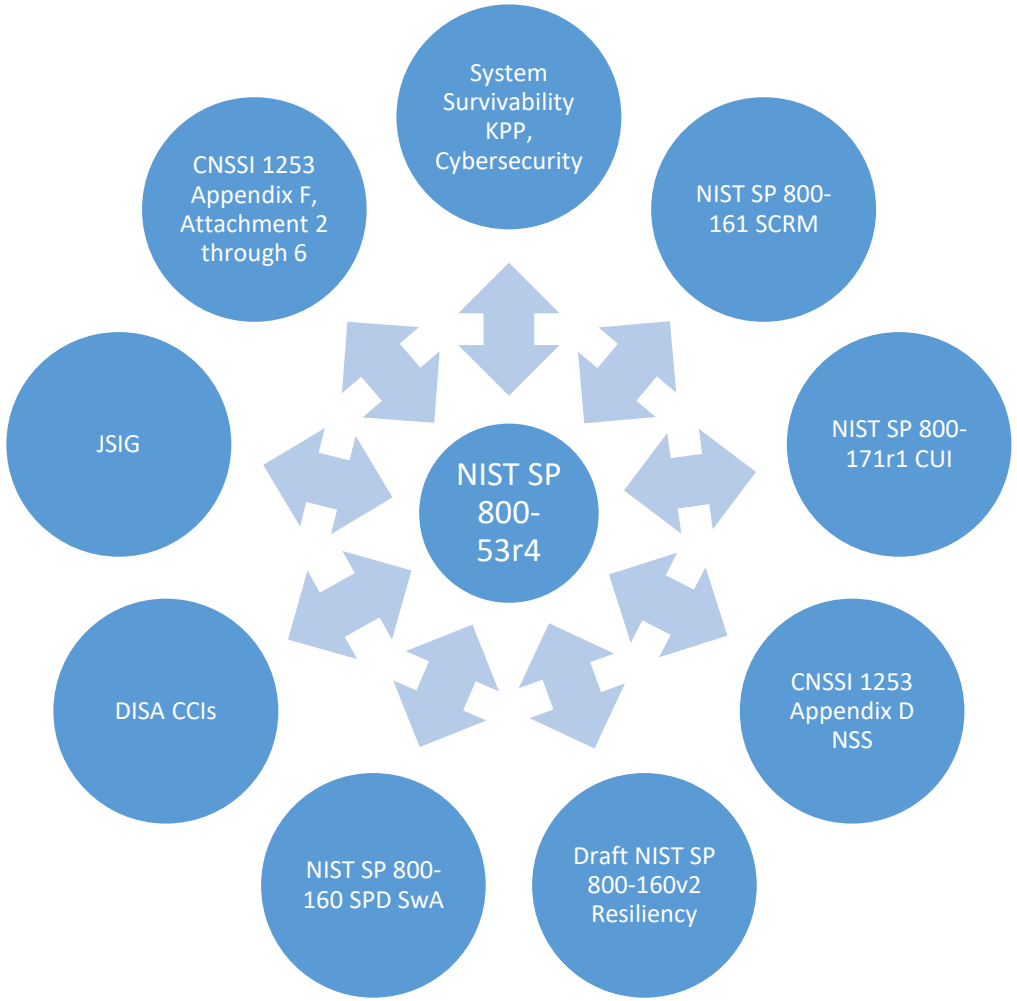
CNSSI 1253 Selects ≈ LLL-311/MMM-403/HHH-478 Requirements
CNSSI 1253 w/Classified ≈ LLL-360/MMM-442/HHH-511 Requirements
CNSSI 1253 w/JSIG ≈ LLL-360/MMM-442/HHH-511 Requirements

THE COMMITTEE ON NATIONAL SECURITY SYSTEMS (CNSS) INSTRUCTION NO. 1253

- **CNSSI 1253, Security Categorization and Control Selection for National Security Systems, 20140327**
  - **Appendix D, NSS Security Control Baselines**
  - **Appendix E, Security Control Parameter Values**
  - **Appendix F, Overlays (control specifications needed to safeguard specific information)**
    - Attachment 1, Overlay Process 20130827
    - Attachment 2, Space Platform Overlay 20130601
    - Attachment 3, Cross Domain Solution Overlay 20130927
    - Attachment 4, Intelligence Community Overlay 20121015 (FOUO document)
    - Attachment 5, Classified Information Overlay 20140509
    - Attachment 6, Privacy Overlay 20150420 (in process)

Exists as DOORS Database linked to NIST SP 800-53r4

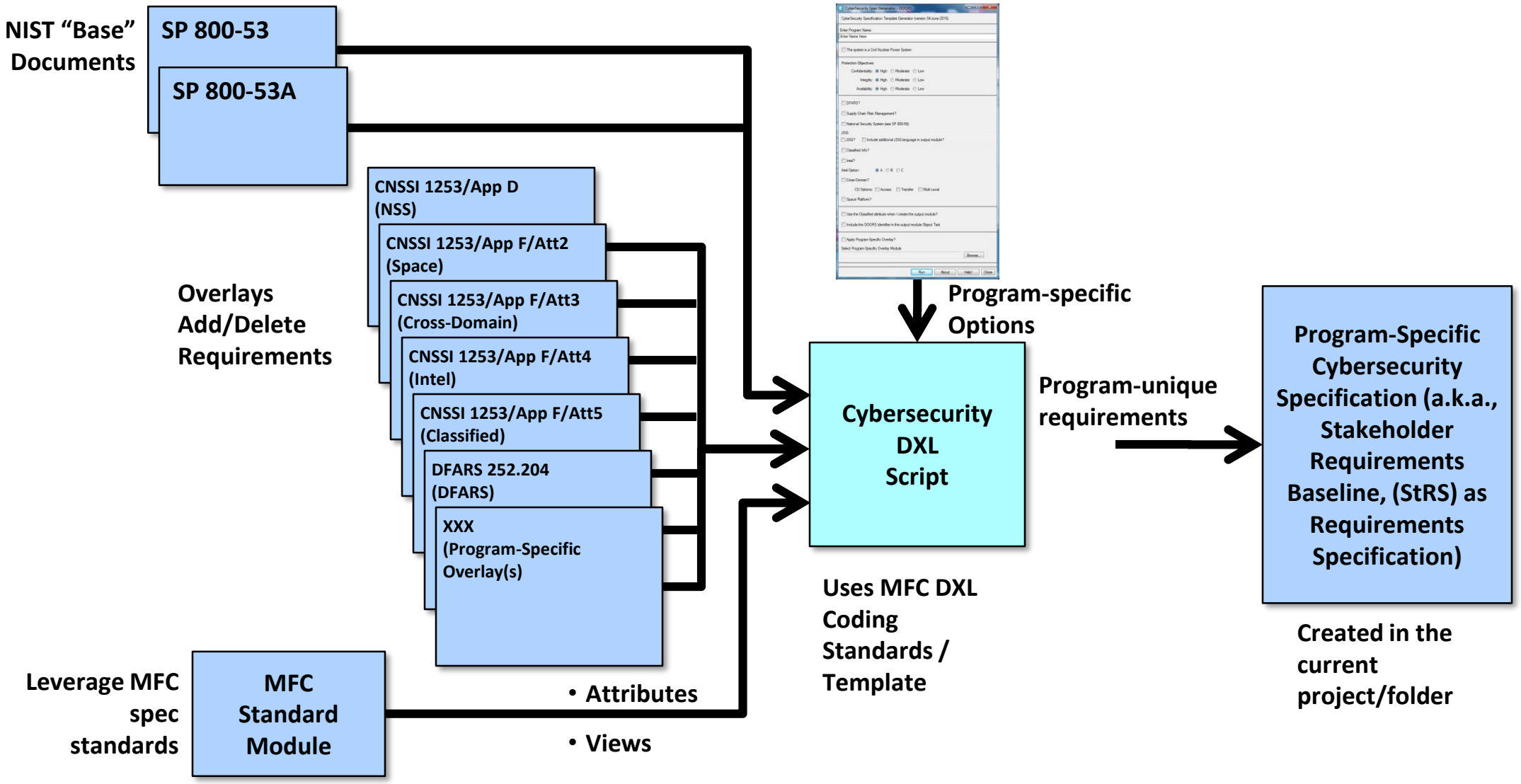
THE NIST SP 800-53R4 HUB AND SPOKES



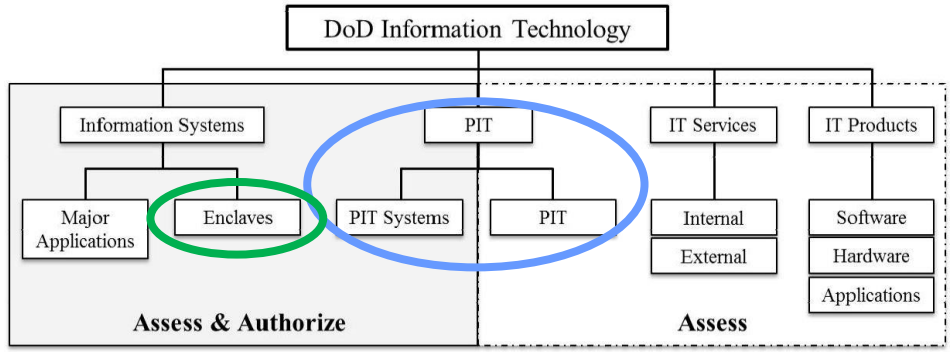
- **NIST SP 800-53r4 is not a Requirements document in and of itself, BUT**
- **Many other documents call for the implementation of Controls and Control Enhancements, or**
- **Other Documents (CCIs) trace to its Controls and Control Enhancements**

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

CYBERSECURITY DOORS DXL SCRIPT OVERVIEW



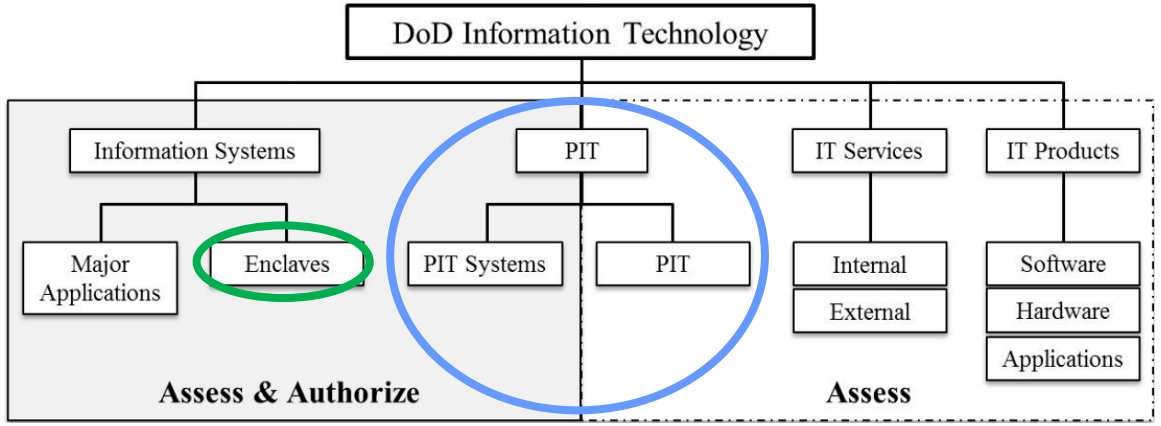
PIT SYSTEMS VS. PIT



- "PIT Systems" are Assessed and Authorized (Dynamic ATO Environment)
  - **Continuing RMF process with IATT as needed and ATOs**
- PIT only requires Assessment (Quasi-static Configuration Environment)
  - **PIT is assessed on a case-by-case basis and apply security controls as appropriate**
  - **Categorize PIT per CNSSI 1253 – tailor the resultant security control baseline (Known Process that Fulfills Requirement)**
  - **PIT is configured per applicable DoD policies and security controls and undergo special assessment of their functional security-related capabilities and deficiencies**
  - **The IS security manager (ISSM) (with the review and approval of the responsible AO) is responsible for ensuring PIT has completed the appropriate evaluation and configuration processes prior to incorporation into or connection to an IS or "PIT system" (Residual Risk Analysis and RAR is MS-B Entrance Criteria)**

PIT Systems – Assess & Authorize (ATO) / PIT – Assess (Formal Configuration Control)

RMF TO PRODUCT AND INFRASTRUCTURE

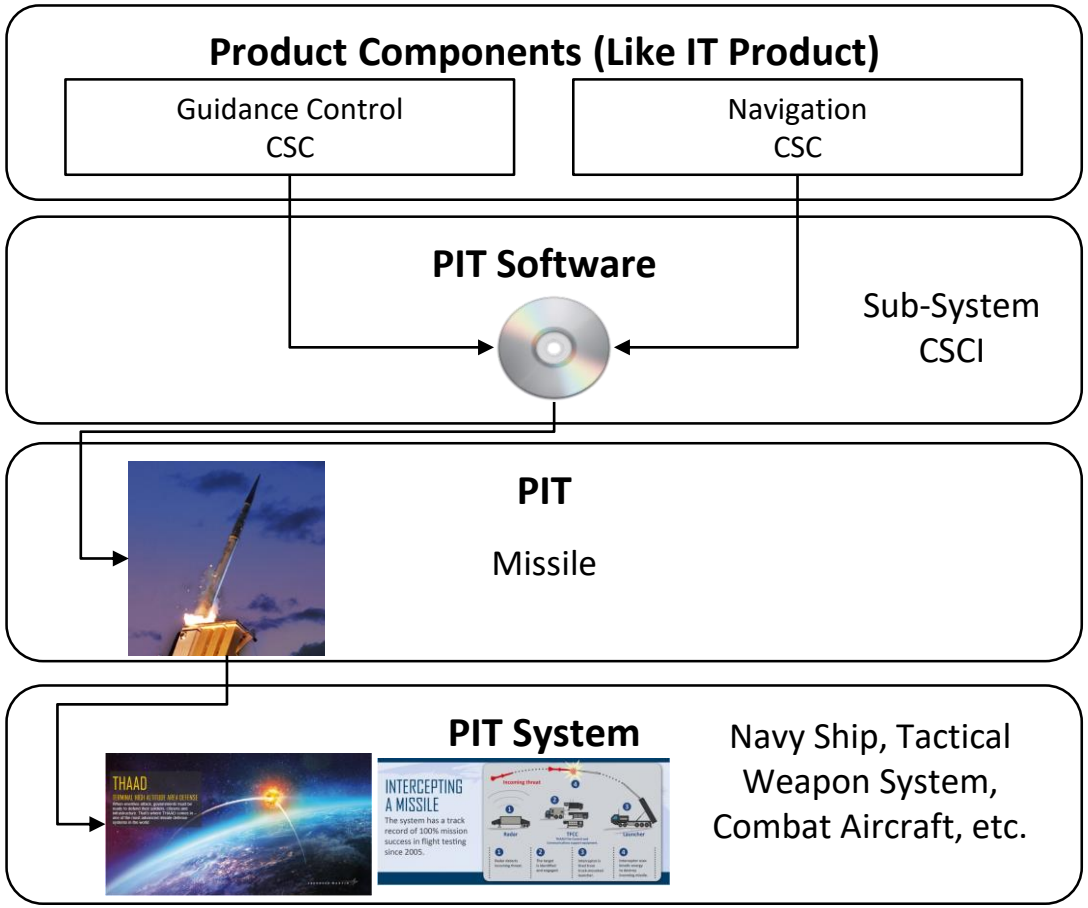


(8510 Encl 3)

Product

Infrastructure

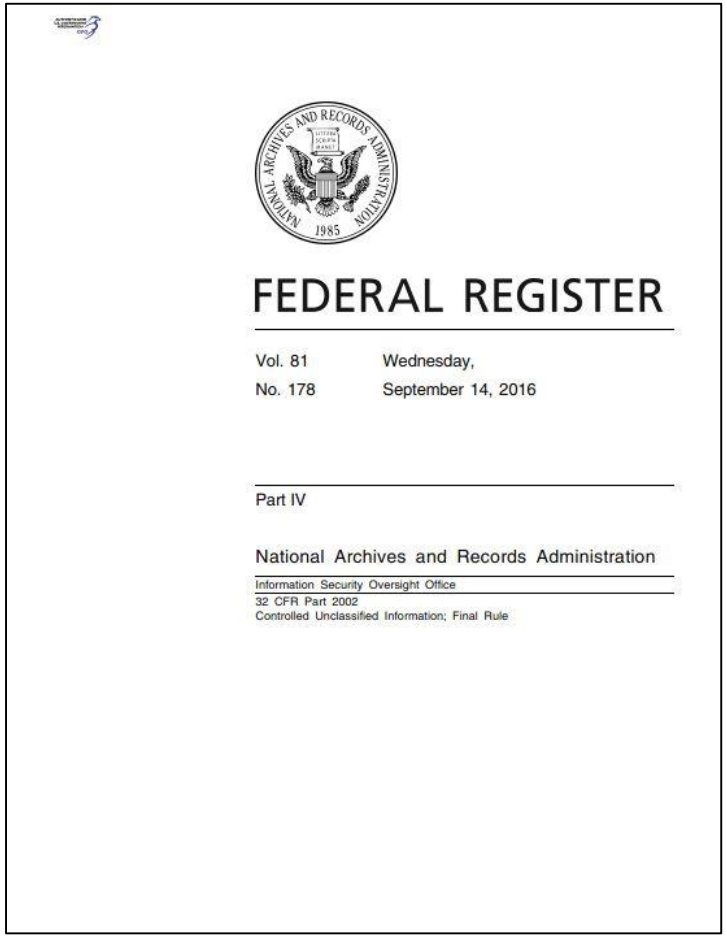
- **Infrastructure**
  - **Enclave for normal business operations**
    - Lockheed Martin Intranet (IT)
  - **Enclave used to develop the product**
    - In LMMFC – Technical Security (Collateral or SAP)
- **Product (PIT/ PIT System)**
  - **PIT assessed, explicit configuration is approved for implementation [Certificate of Conformance, looks like a Security Technical Implementation Guide (STIG)]**
    - Example – Hellfire II, SNIPER
  - **PIT System- requires IATT and ATOs**
    - Example – THADD (Tactical Weapon System)
  - **In LMMFC – Cybersecurity Engineering**



LMMFC Products are PIT or PIT Systems

32CFR2002
CONTROLLED UNCLASSIFIED INFORMATION FINAL RULE

- As the Federal Government's Executive Agent (EA) for Controlled Unclassified Information (CUI), the National Archives and Records Administration (NARA), through its Information Security Oversight Office (ISOO), oversees the Federal Government-wide CUI Program.
- This rule is effective November 14, 2016
- § 2002.2 Incorporation by reference
  - **FIPS PUB 199**
  - **FIPS PUB 200**
  - **NIST SP 800-53r4**
  - **NIST SP 800-88r1**
  - **NIST SP 800-171**



FEDERAL REGISTER

Vol. 81 Wednesday,
No. 178 September 14, 2016

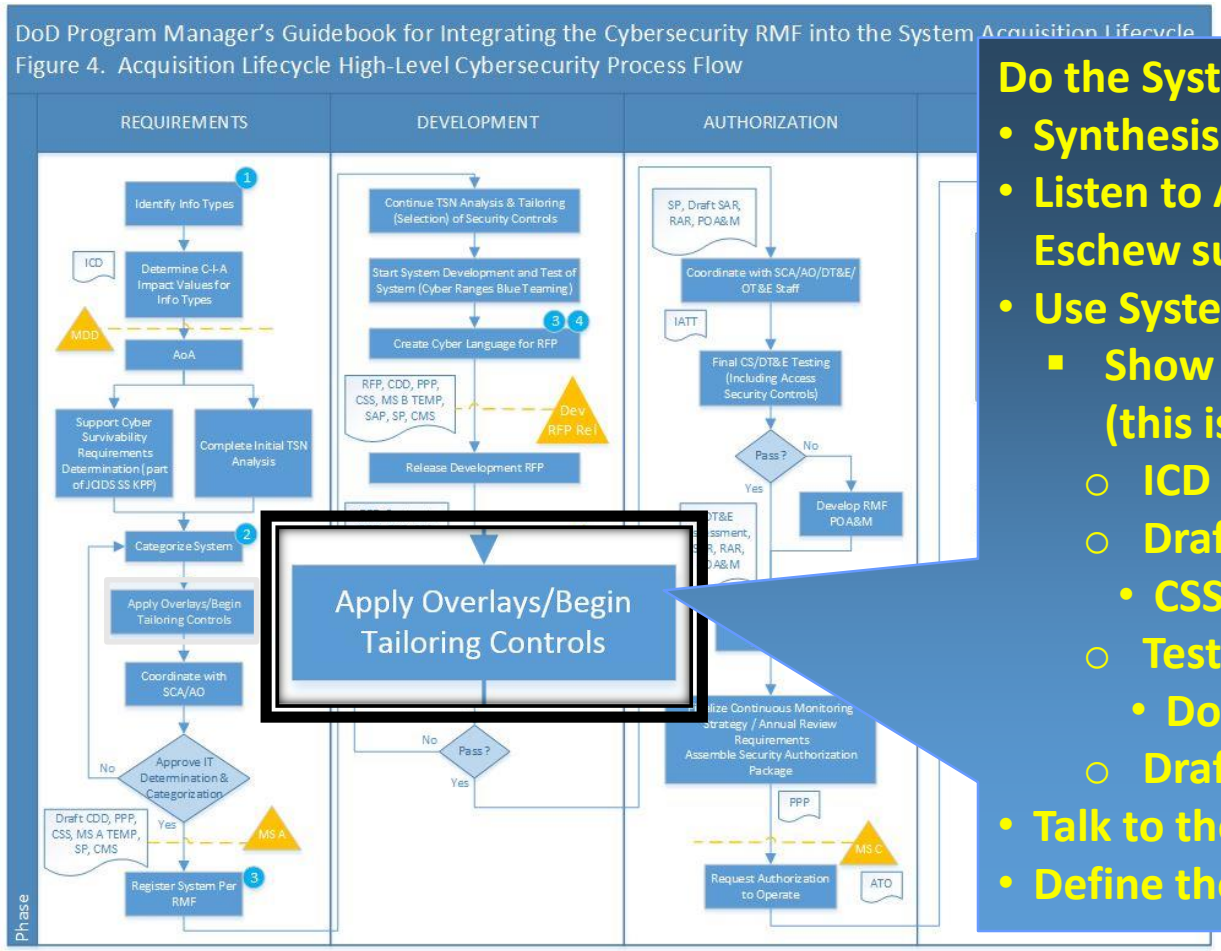
Part IV

National Archives and Records Administration

Information Security Oversight Office
32 CFR Part 2002
Controlled Unclassified Information; Final Rule

NIST SP 800-171 is a "Federal Regulation"

INTEGRATING RMF INTO DoD ACQUISITION: IRAD WORK, PRE-MILESTONE A (MS A)

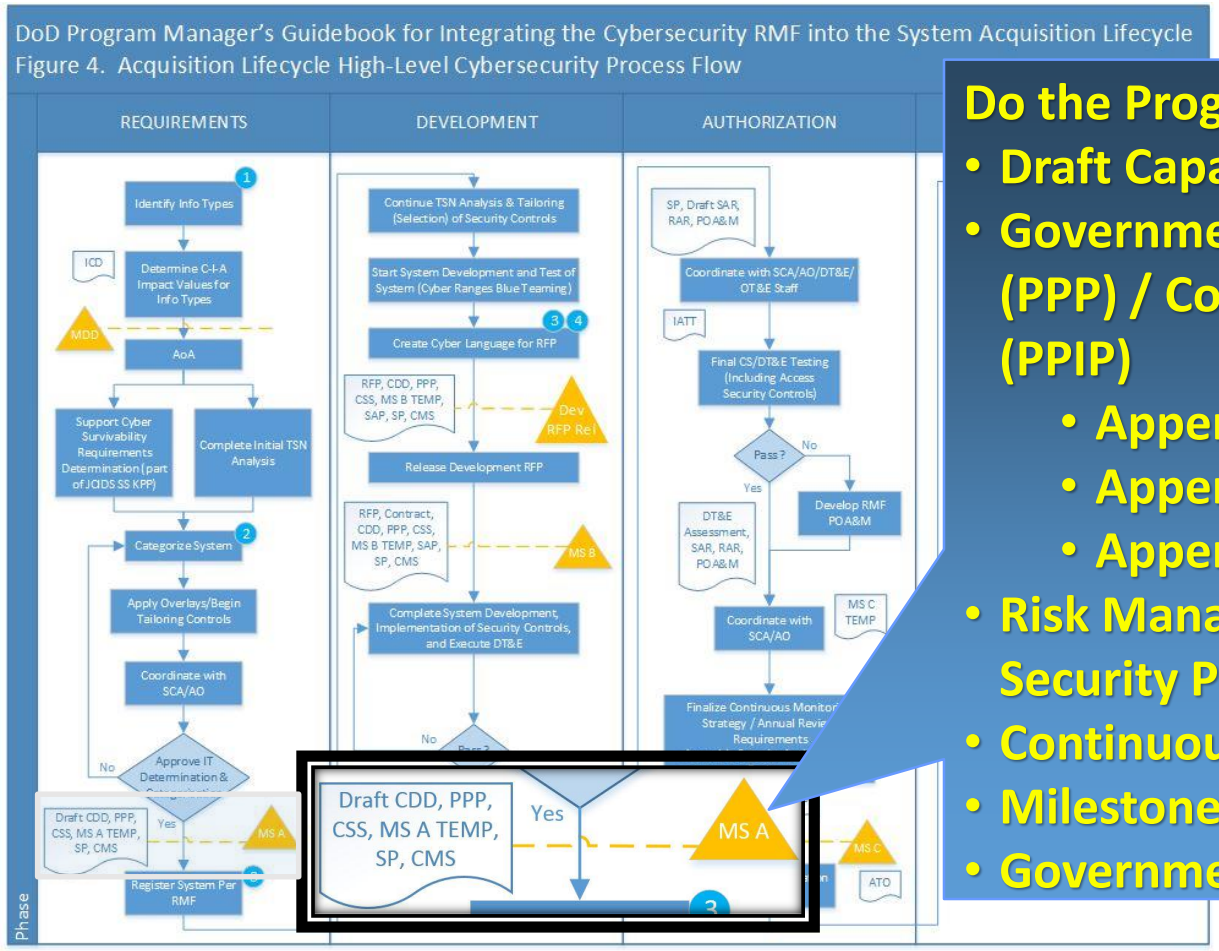


Do the Systems Engineering

- **Synthesis is Work, not a Buzz-word**
- **Listen to Arthur D. Hall III, be Affordable; Eschew sub-optimization**
- **Use Systems Engineering, shape the TMRR RFP:**
  - **Show Bi-Directional Traceability (this is Required by DoDI 5000.02)**
    - **ICD to Draft CDD (Cybersecurity is in SS KPP)**
    - **Draft CDD to PPP to PPIP**
      - **CSS and AT Plan are App to PPP**
    - **Test and Evaluation Master Plan (TEMP)**
      - **DoD Cybersecurity T&E Guidebook**
    - **Draft Continuous Monitoring Strategy**
- **Talk to the Customer Stakeholder**
- **Define the Stakeholder Req. Spec. (StRS)**

Guide the Customer to the MS A answer

INTEGRATING RMF INTO DoD ACQUISITION: IRAD WORK, PRE-MILESTONE A (MS A)



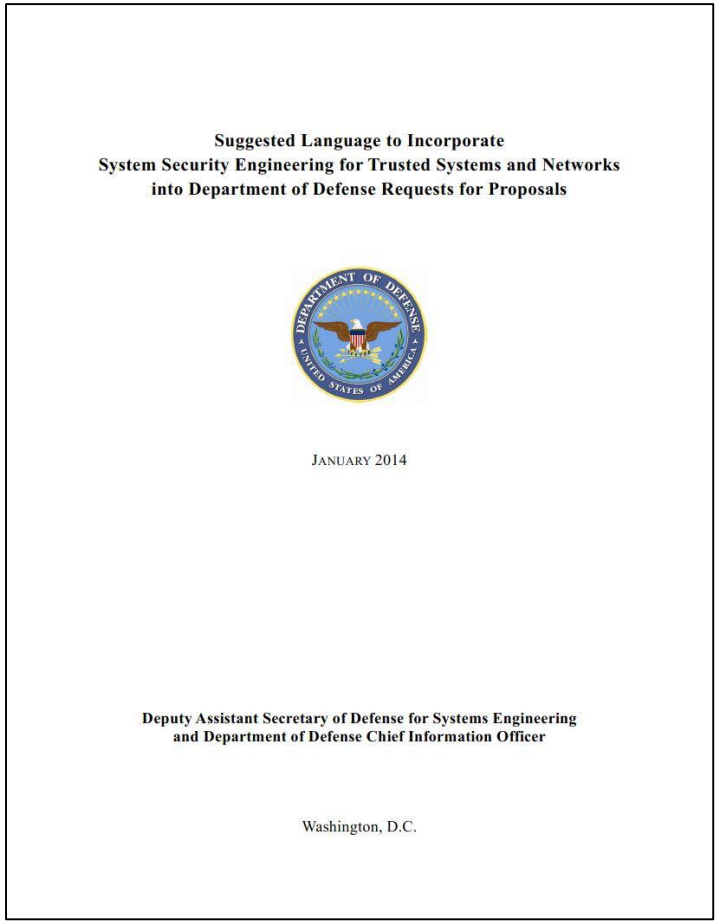
Do the Program / Systems Engineering Work

- **Draft Capability Development Document (CDD)**
- **Government Program Office (GPO) Program Protection Plan (PPP) / Contractor Program Protection Implementation Plan (PPIP)**
  - **Appendix C: Criticality Analysis (CPI and CC)**
  - **Appendix D: Anti-Tamper Plan**
  - **Appendix E: Cybersecurity Strategy**
- **Risk Management Framework (RMF) Security Plan (SP) (a.k.a., "Specification")**
- **Continuous Monitoring Strategy (CMS)**
- **Milestone A (MS-A) Test and Evaluation Master Plan (TEMP)**
- **Government Program Office RFP / Contractor Bid Package**

This Work Defines the Stakeholder Requirements Baseline

OSD SYSTEMS ENGINEER/DoD CIO SUGGESTED RFP LANGUAGE

- This document is intended for use by Department of Defense (DoD) program managers preparing requests for proposals (RFP) for major defense acquisitions. Notes in italics are directions to the program office and are not to be included in the RFP.
- This RFP language implements the policy outlined in Department of Defense Instruction (DoDI) 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks," **only**. This language does not address critical program information (CPI), anti-tamper, or defense exportability.
- The program office should tailor this RFP language based on the cost-benefit analysis for each acquisition.
- Language by Section:
  - **Section C: Statement of Work**
  - **Section C: System Requirements Document**
  - **Section L: Instructions, Conditions, and Notices to Offerors**
  - **Section M: Proposal Evaluation Criteria**



Suggested Language to Incorporate
System Security Engineering for Trusted Systems and Networks
into Department of Defense Requests for Proposals

JANUARY 2014

Deputy Assistant Secretary of Defense for Systems Engineering
and Department of Defense Chief Information Officer

Washington, D.C.

We Write Standard Answers to Standard RFPs

OSD SYSTEMS ENGINEER/DoD CIO SOFTWARE ASSURANCE COUNTERMEASURES

Software Assurance Countermeasures in Program Protection Planning

MARCH 2014

Deputy Assistant Secretary of Defense for Systems Engineering and Department of Defense Chief Information Officer

Washington, D.C.

Development Process								
Software (CPI, critical function components, other software)	**Static Analysis p/a (%)**	**Design Inspect**	**Code Inspect p/a (%)**	**CVE p/a (%)**	**CAPEC p/a (%)**	**CWE p/a (%)**	**Pen Test**	**Test Coverage p/a (%)**
Developmental CPI SW	100/80	Two Levels	100/80	100/60	100/60	100/60	Yes	75/50
Developmental Critical Function SW	100/80	Two Levels	100/80	100/70	100/70	100/70	Yes	75/50
Other Developmental SW	none	One level	100/65	10/0	10/0	10/0	No	50/25
COTS CPI and Critical Function SW	Vendor SwA	Vendor SwA	Vendor SwA	0	0	0	Yes	UNK
COTS (other than CPI and Critical Function) and NDI SW	No	No	No	0	0	0	No	UNK

Operational System						
	Failover Multiple Supplier Redundancy (%)	**Fault Isolation**	**Least Privilege**	**System Element Isolation**	**Input Checking / Validation**	**SW Load Key**
Developmental CPI SW	30	All	all	yes	All	All
Developmental Critical Function SW	50	All	All	yes	All	all
Other Developmental SW	none	Partial	none	None	all	all
COTS (CPI and CF) and NDI SW	none	Partial	All	None	Wrappers/ all	all

Development Environment								
SW Product	**Source**	**Release Testing**	**Generated Code Inspection p/a (%)**					
C Compiler	No	Yes	50/20					
Runtime libraries	Yes	Yes	70/none					
Automated test system	No	Yes	50/none					
Configuration management system	No	Yes	NA					
Database	No	Yes	50/none					
Development Environment Access	Controlled access; Cleared personnel only							

FIGURE 1 – SOFTWARE ASSURANCE COUNTERMEASURES (SAMPLE)

- The purpose of the software assurance countermeasures section of the Program Protection Plan (PPP) is to help programs develop a plan and statement of requirements for software assurance early in the acquisition lifecycle and to incorporate the requirements into the request for proposal (RFP).
- The progress toward achieving the plan is measured by actual accomplishments/results that are reported at each of the Systems Engineering Technical Reviews (SETR) and recorded as part of the PPP.

Software Assurance and the "Terrible Table"

As Paul Harvey would say at the end; and now you know the rest of the story.
Not quite the way he used the phrase, but …

"CYBERSECURITY THE SYSTEMS ENGINEERING WAY"

CORELATED ENCLAVE TO PIT SYSTEM / PIT WORK PRODUCTS

Enclave Work Products (Stove-Pipe)

- **Cybersecurity Strategy**
- **System Security Plan (SSP) (RMS KS)**
  - **Ports, Protocols, & Services Management**
  - **DoD Security Control Set**
  - **System Authorization Boundary**
- **Continuous Monitoring Strategy (CMS) (NIST SP 800-137 ISCM)**
- **Security Assessment Plan (SAP)**
- **Security Assessment Report (SAR)**
- **Risk Assessment Report (RAR)**
- **Plan of Action and Milestones (POA&M)**

PIT System / PIT Work Products (Integrated)

- **PPP/PPIP at Appendix E (DoD CIO memo of 20151110 w/template)**
- **System Requirements Specification (SyRS), etc., flow-down Spec.**
  - **§2 Applicable Documents (Internal/External ICDs tied to §6.1 DoDAF SV-1, SV-3)**
  - **§3 Requirements (against HWCI/CSCI Critical Component from PPIP Appendix C) with System-of-Interest C-I-A & Overlays (from NIST SP 800-53r4 and associated CCIs)**
  - **§6.1 Intended Use (to include DoDAF OV-1 High-Level Operational Concept Graphic, DoDAF SV-1 Systems Interface Description, and SV-3 Systems-Systems Matrix)**
- **Cybersecurity Section of SEMP (Tier 1 and/or 2), SyRS §6.1 Intended Use (System-of-Interest Tier 3 Strategy) and PPIP**
- **TEMP Cybersecurity Section & SyRS (w/flow-down) §4 Verification**
- **SyRS (w/flow-down)§4 Verification Reports**
- **Pre MS-A & B Analysis Reports (Design Residual Risk) and Cybersecurity Section of DT&E/OT&E for Requirement Compliance**
  - **Note, the 15288/800-160 (§6.4.2.3e/§3.4.2 SN-5) Analyze Stakeholder Security Requirements Report "Defines" Design SySR Residual Risk for System-of-Interest**
- **Engineering Change Proposal (ECP) / Preplanned Product Improvement (P3I)**

PIT Acquisition Systems Engineering Includes Enclave "Stove-Pipe" Work Products

CYBERSECURITY IN DoD ACQUISITION OF DEVELOPMENTAL CONFIGURATION ITEMS (I.E., PIT MATERIEL PROCUREMENT)

- Recognize the need for Security within the System-of-Interest (i.e., PIT) at MDD
- Include Cybersecurity (and other Security, e.g., AT, SwA, SCRM) with all the other System-of-Interest Requirements (System Survivability KPP)
- For National Security Systems (NSS a.k.a., weapons, etc.) execute CNSSI 1253 Chapter 3
- Between Alternative System Review (ASR) and System Requirements Review (SRR) resolve Competing and Conflicting Requirements (Required Requirements Engineering)
  - **Publish System-of-Interest System Requirements Specification (SyRS)**
  - **The Cybersecurity Competing and Conflicting Requirements Analysis Report Defines the System-of-Interest (SoI) "Residual Risk" and requires AO/ISSM Approval**
    - Milestone B Entrance Criteria (RMF Step 2+ (Select), vice waiting to RMF Step 5 (Authorize))
    - The SoI "Residual Risk" report is analogous to an Enclave Risk Assessment Report (RAR)
      - P3I or ECP addresses SoI Non-compliance (POA&M addresses Enclave vulnerabilities)
  - **All SyRS Requirements will be "Compliant" and "Verified" (SyRS §4 Verification)**
- Follow the normal DoD Acquisition Process to obtain a Compliant SoI

Built In Cybersecurity using Requirements Engineering is the only Affordable Solution

TADIC-P OR TEST, ANALYSIS, DEMONSTRATION, INSPECTION, CERTIFICATION, AND PROCESS

- **Test** – The exercise of hardware, software, and/or operations under specified and controlled conditions using procedures and instrumentation/measuring equipment to verify compliance with quantitatively specified requirements.
- **Analysis or simulation** – Technical evaluation of data using logic, mathematics, modeling, simulation, or analysis techniques under defined conditions to determine compliance with requirements.
- **Demonstration** – The un-instrumented (i.e., special test instrumentation, not the normal delivered system-of-interest self-monitoring instrumentation) exercise of hardware, software, or operations to determine by observation the qualitative performance of specified functions.
- **Inspection** – Examination by the senses (sight, sound, smell, taste, or touch) without the use of special equipment to determine requirements compliance. The NIST SP 800-53Ar4 “Examine” and “Interview” verification methods are special case examples of Inspection.
- **Certification** – When an outside authority (e.g., Underwriter's Laboratory, UL) performs the validation activity to determine requirements compliance and provides a "certification" to that effect.
- **Process** – The case where the evidence of requirement compliance derives from a defined special process because TADIC as defined above cannot verify the requirement. A special process is “a process, the results of which are highly dependent on the control of the process or the skill of the operators, or both, and in which the specified quality cannot be readily determined by inspection or test of the product” (i.e., system-of-interest). (ASME NQA-1-2008/ASME NQA-1a-2009, Part I, §400 Terms and Definitions)

SYSTEM SECURITY SYSTEMS ENGINEERING

MEC CYBER SECURITY

SYSTEMS ENGINEERING