

The background of the slide is a dark blue field filled with a complex, glowing circuit pattern. The circuit lines are primarily light blue and white, with some segments highlighted in green and orange. The pattern consists of numerous interconnected lines, loops, and nodes, creating a dense, technical aesthetic that resembles a printed circuit board or a digital network map.

Cybersecurity in Transition

Next Gen Security Frameworks, Controls, and Engineering

Agenda



NIST Controlled Unclassified Information (CUI) Series



Special Publication (SP) 800-53 Security & Privacy Controls



System Security Engineering Guidance



Applied Research at the NCCoE

The NIST CUI Series

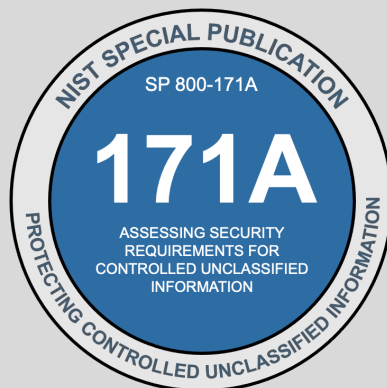


Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations



CUI Security Requirements

Protect the **confidentiality** of CUI in nonfederal systems and organizations



Assessment Procedures for CUI Security Requirements

Assessment methodology and procedures for the SP 800-171 CUI security requirements



Enhanced Security Requirements for Protecting CUI

Supplement to SP 800-171 to address **advanced persistent threat** in critical programs and high value assets



Assessment Procedures for Enhanced Security Requirements

Assessment procedures for the SP 800-172 enhanced security requirements

The Development of the CUI Series

2013

2015

2016

2018

2020

2021

2022

2013

NIST, DOD and NARA begin work on what will become SP 800-171

June 2015

SP 800-171 published*

Dec 2016

SP 800-171 Rev. 1 published*

June 2018

SP 800-171A published*

Feb 2020

SP 800-171 Rev. 2 published*

Feb 2021

SP 800-172 published*

March 2022

SP 800-172A published*

April 2022

CSV & spreadsheet of SP 800-171 series published (requirements & assessment procedures)

SP 800-171 Rev. 1. added requirement for & guidance on system security plans

Draft SP 800-171A introduced "Discussion" section for each CUI security requirement

SP 800-171 Rev. 2 included "Discussion;" no substantive changes to requirements

SP 800-172 allowed the federal agency to select which enhanced security requirements apply

2013

Safeguarding of Unclassified Controlled Technical Information DFARS published

2015

DFARS rule revised to cite SP 800-171 and apply broadly to DOD CUI

2016

NARA CUI Federal Rule (32 CFR 2002) published

2018

NIST, in collaboration with NARA and DOD, held workshop on CUI Security Requirements

2019

DOD announced creation of the CMMC

2021

DOD announced CMMC 2.0

Pre-Call for Comments



NIST seeks feedback about the use, effectiveness, adequacy, and ongoing improvement of the **CUI series.**

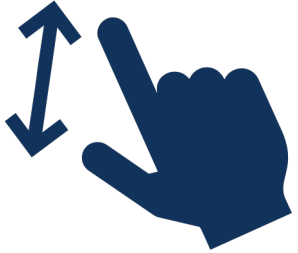
Submit your feedback to
800-171comments@list.nist.gov
by September 16, 2022

Comments received in response to this request will be posted on the [Protecting CUI project site](#).

Submitters' names and affiliations (when provided) will be included, while contact information will be removed.

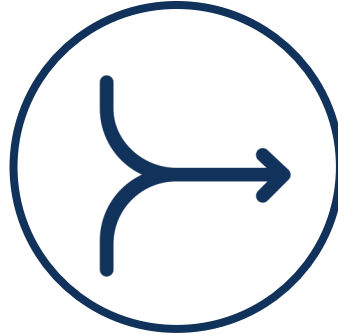
<https://csrc.nist.gov/publications/detail/sp/800-171/rev-3/draft>

Seeking your feedback on



Use of the CUI Series

- Current use of the CUI series alone or with other frameworks and standards
- How to improve alignment
- Benefits and challenges



Updates for Consistency with SP 800-53 Rev 5

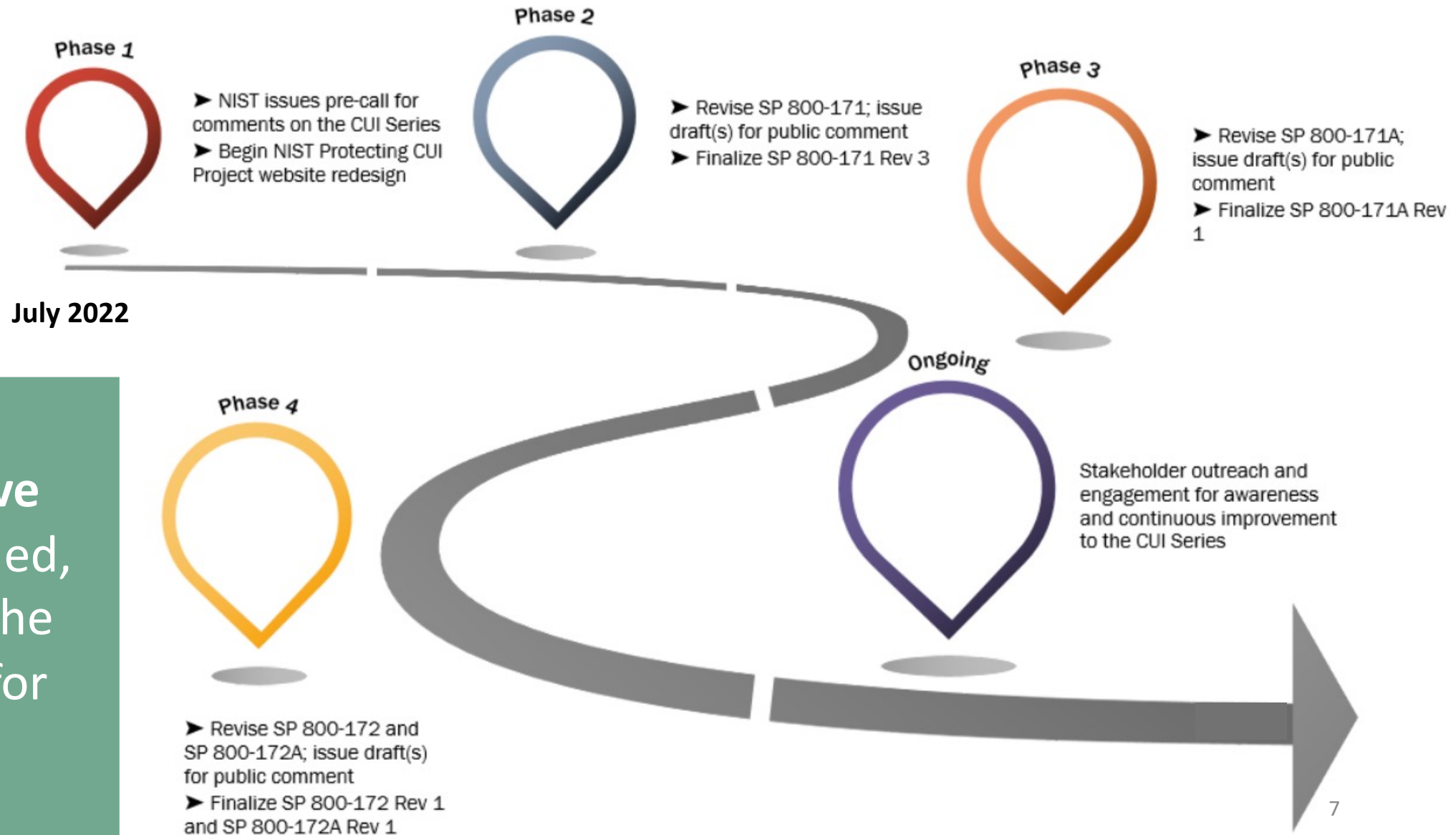
- Impact on usability and existing implementations



Updates to Improve Usability and Implementation

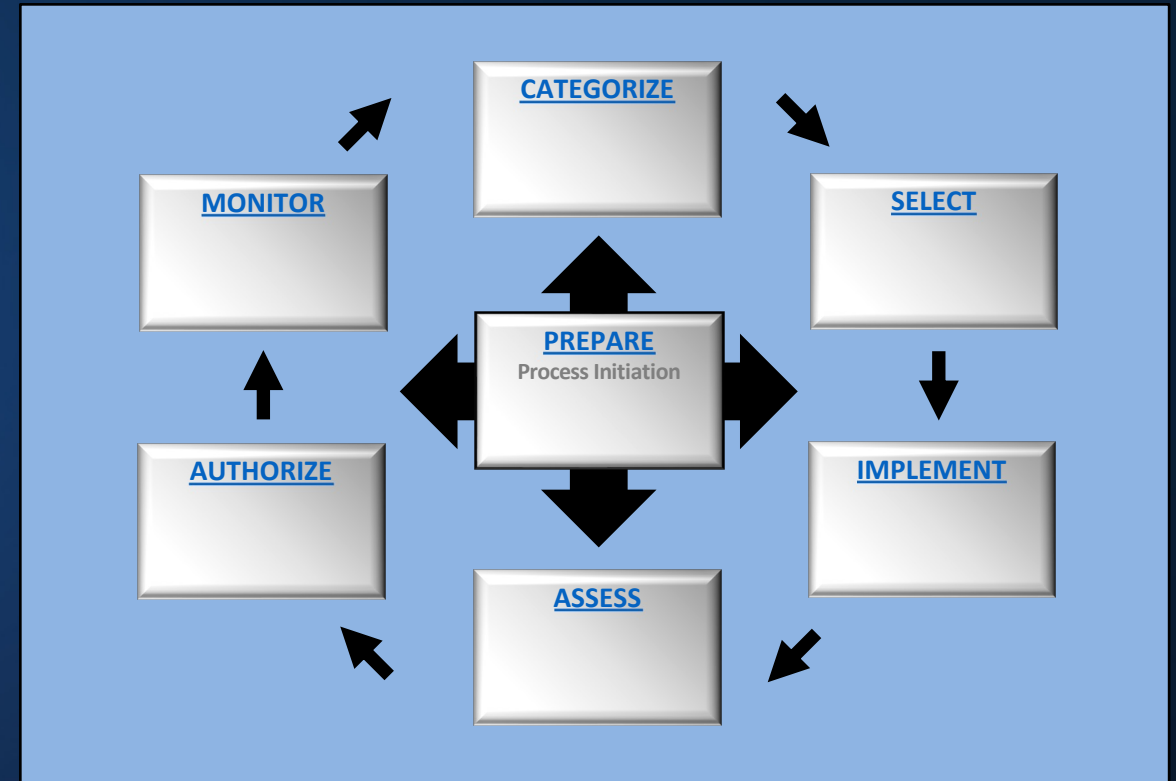
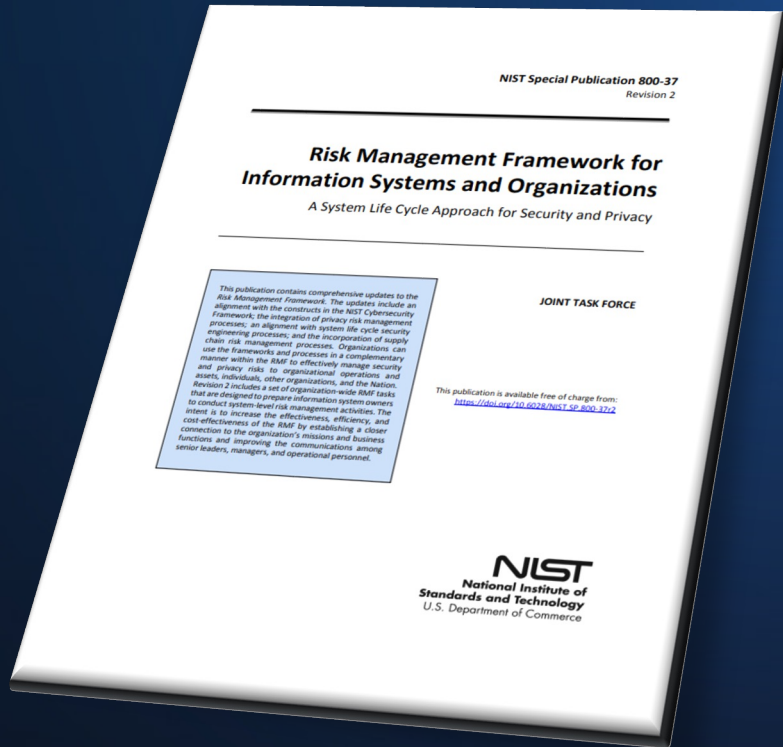
- Features to change, add, or remove
- Any additional ways to improve

Looking Ahead for the CUI Series



Comprehensive updates planned, starting with the pre-draft call for comments

Managing Risk in Systems and Organizations

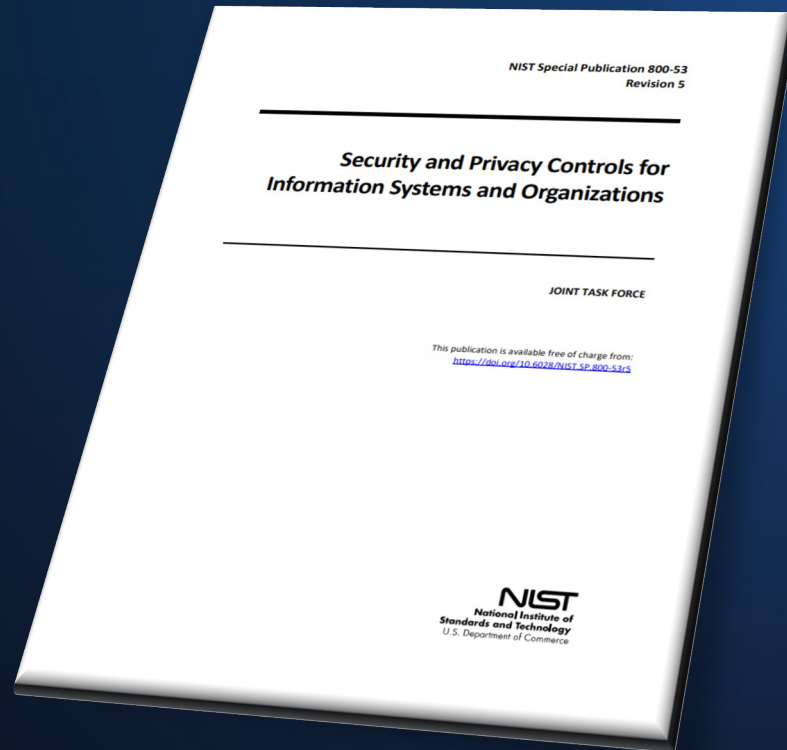


Courtesy: NIST Special Publication 800-37, Revision 2

- New control selection process supports general-purpose and specialized systems

<https://csrc.nist.gov/projects/risk-management>

Security and Privacy Controls



ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
CP	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Courtesy: NIST Special Publication 800-53, Revision 5

- New privacy control family and privacy integration throughout the control catalog
- New supply chain risk management control family
- Systems security engineering controls
- New state-of-the-practice controls to counter advanced threats

NIST SP 800-53 Security & Privacy Controls at a glance



CATALOG OF
**SECURITY &
PRIVACY** CONTROLS



USED AS PART OF A
**RISK
MANAGEMENT**
PROCESS



APPLICABLE TO
ALL TYPES
OF SYSTEMS &
ORGANIZATIONS



6 REVISIONS SINCE
2005



INTERNATIONAL
USE AND IMPACT



AVAILABLE IN
**MULTIPLE DATA
FORMATS**



ASSESSMENT
PROCEDURES
SP 800-53A

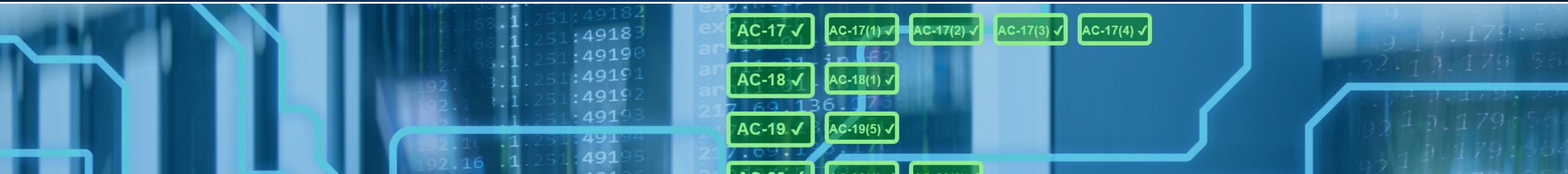


CONTROL BASELINES
SP 800-53B



SUBMIT YOUR
COMMENTS
24/7

Controls, Baselines & Assessment



Security & Privacy Controls for Systems & Organizations

- Catalog of **security & privacy controls**
- **Outcomes** that can be selected / implemented to manage risk
- Applicable to **any type of system** (i.e., IoT, OT, enterprise)

SP 800-53 Rev. 5

Control Baselines for Systems & Organizations

- **3 security control baselines** – Low, Moderate, and High
- **New privacy control baseline**
- Tailoring & overlay guidance

SP 800-53B

Assessing Security & Privacy Controls in Systems & Orgs

- Methodology and customizable procedures for **conducting assessments of SP 800-53 controls**
- Information on building **effective assessment plans**

SP 800-53A Rev. 5

Summary of Changes: SP 800-53 Rev 5



- Separation of **controls** from the **process**
- Controls are more **outcome-focused**



- Privacy and Supply Chain Risk Management controls added to the Program Management (PM) Family & incorporated into applicable controls throughout
- New Control Families:
 - Personally Identifiable Information Processing and Transparency (PT)
 - Supply Chain Risk Management (SR)



- Control baselines, overlay & tailoring guidance **moved to SP 800-53B**
- Mappings and control keywords posted as **supplemental materials**

Summary of Changes: SP 800-53B

CONTROL NUMBER	CONTROL NAME <small>CONTROL ENHANCEMENT NAME</small>	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PL-8	Security and Privacy Architectures	x		x	x
PL-8(1)	DEFENSE-IN-DEPTH				
PL-8(2)	SUPPLIER DIVERSITY				
PL-9	Central Management	x			
PL-10	Baseline Selection		x	x	x

Security Control Basslines (L, M, H)

- Minor updates between SP 800-53 Revision 4 and 800-53B

NEW Privacy Control Baseline

- Initial privacy control baseline to address **privacy requirements** and manage privacy risks from the **processing of PII based on privacy program responsibilities under OMB Circular A-130**
- Independent of the security control baselines

Changes Between SP 800-53 Rev 4 & 5



Rev 5 Update	NIST SP 800-53 Rev 5 Controls	NIST SP 800-53B Control Baselines				More than editorial or administrative change? (Y/N)	Changed Elements	Change Details
AT-3	Role-Based Training	X	X	X	X	Y	Changes title Changes control text Adds parameter Changes discussion Adds to Privacy Control Baseline (SP 800-53B)	privacy incidents into training Adds parameter requiring role-based security and privacy training for personnel with specific roles and responsibilities Adds new control text with a parameter to update role-based training at a specific frequency Discussion adds examples of personnel to be trained as well as events that may precipitate an update to role-based training Incorporates role-based training elements of withdrawn App J control AR-5
AT-3(1)	Role-Based Training Environmental Controls					N	Changes discussion	Does not change intent
AT-3(2)	Role-Based Training Physical Security Controls					N	Changes discussion	Does not change intent
AT-3(3)	Role-Based Training Practical Exercises					Y	Adds control text Changes discussion	Adds privacy to control text, to imply training includes privacy, as well as security Discussion expanded to include examples of practical exercises for privacy
AT-3(4)	<i>Role-Based Training Suspicious Communications and Anomalous System Behavior</i>					Y	Withdrawn	Moved to AT-2(4)
AT-3(5)	Role-Based Training Processing Personally Identifiable Information	X				Y	New control enhancement Adds to Privacy Control Baseline (SP 800-53B)	Provide specific personnel or roles with initial and at a specific frequency training in the employment and operation of PII processing and transparency controls Incorporates training elements of withdrawn App J control UL-2
AT-4	Training Records	X	X	X	X	Y	Changes title Changes control text Changes discussion Adds to Privacy Control Baseline (SP 800-53B)	Title changed from 'Security Training Records' Adds privacy to control text, to imply training includes privacy, as well as security Discussion includes reference to NARA
AT-5	<i>Contacts With Security Groups and Associations</i>					N	N	Previously withdrawn in Rev4; Incorporated into PM-15

Thank you to MITRE Corporation & Director of National Intelligence for sharing a spreadsheet analysis of control changes

NIST SP 800-53 Rev. 5 & SP 800-53B

CA-5 PLAN OF ACTION AND MILESTONES

Control:

- Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and
- Update existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

Discussion: Plans of action and milestones are useful for any type of organization to track planned remedial actions. Plans of action and milestones are required in authorization packages and subject to federal reporting requirements established by OMB.

Related Controls: [CA-2](#), [CA-7](#), [PM-4](#), [PM-9](#), [RA-7](#), [SI-2](#), [SI-12](#).



	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
CA-1	Policy and Procedures	X	X	X	X
CA-2	Control Assessments	X	X	X	X
CA-2(1)	INDEPENDENT ASSESSORS			X	X
CA-2(2)	SPECIALIZED ASSESSMENTS				X
CA-2(3)	LEVERAGING RESULTS FROM EXTERNAL ORGANIZATIONS				
CA-3	Information Exchange		X	X	X
CA-3(1)	UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	W: Moved to SC-7(25).			
CA-3(2)	CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	W: Moved to SC-7(26).			

SP 800-53 Rev 5.1 and SP 800-53B Latest Versions

CA-5 PLAN OF ACTION AND MILESTONES

Family:	CA - ASSESSMENT, AUTHORIZATION, AND MONITORING		
	Low	Moderate	High
Security Baseline:	CA-5	CA-5	CA-5
Privacy Baseline:	CA-5		

Jump To:

[All Controls](#) > [CA](#) > [CA-5](#)

Jump To:

[REVISION 5.1](#)

[Home](#)
[Control Families](#)
[Low-Impact](#)
[Moderate-Impact](#)
[High-Impact](#)
[Privacy Control Baseline](#)
[All Controls](#)
[Search](#)

Control

- Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and



```
3917 <title>Plan of Action and Milestones</title>
3918 <param id="ca-05_odp">
3919   <prop name="alt-identifier" value="ca-5_prm_1"/>
3920   <prop name="label" class="sp800-53a" value="CA-05_ODP"/>
3921   <label>frequency</label>
3922   <guideline>
3923     <p>the frequency at which to update an existing plan of action and milestones based on the findings from control assessments, independent audit
3924   </guideline>
3925 </param>
3926 <prop name="label" value="CA-5"/>
3927 <prop name="label" class="sp800-53a" value="CA-05"/>
3928 <prop name="sort-id" value="ca-05"/>
3929 <link rel="reference" href="#27847491-5ce1-4f6a-a1e4-9e483782f0ef"/>
3930 <link rel="reference" href="#482e4c99-9dc4-41ad-bba8-0f3f0032c1f8"/>
3931 <link rel="related" href="#ca-2"/>
3932 <link rel="related" href="#ca-7"/>
3933 <link rel="related" href="#pm-4"/>
3934 <link rel="related" href="#pm-9"/>
3935 <link rel="related" href="#ra-7"/>
3936 <link rel="related" href="#si-2"/>
3937 <link rel="related" href="#si-12"/>
3938 <part name="statement" id="ca-5_smt">
3939   <part name="item" id="ca-5_smt.a">
3940     <prop name="label" value="a"/>
3941     <p>Develop a plan of action and milestones for the system to document the planned remediation actions of the organiza
3942   </part>
3943   <part name="item" id="ca-5_smt.b">
```

OSCAL

Summary of Changes: SP 800-53A Rev. 5



UPDATED ASSESSMENT PROCEDURES
CORRESPOND W/ SP 800-53 REV 5 CONTROLS



FIRST SET OF
PROCEDURES FOR
PRIVACY CONTROLS



UPDATED ASSESSMENT
PROCEDURE STRUCTURE

NIST SP 800-53A Rev. 5

CA-05	PLAN OF ACTION AND MILESTONES	
	ASSESSMENT OBJECTIVE: <i>Determine if:</i>	
CA-05_ODP	<i>the frequency at which to update an existing plan of action and milestones based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities is defined;</i>	
CA-05a.	a plan of action and milestones for the system is developed to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system;	
CA-05b.	existing plan of action and milestones are updated on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.	
POTENTIAL ASSESSMENT METHODS AND OBJECTS:		
CA-05-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; assessment report; control assessment evidence; control assessment plan; system security plan; privacy plan; other relevant information]	
CA-05-Interview	[SELECT FROM: Organizational personnel with plan development and implementation responsibilities; information security and privacy responsibilities]	
CA-05-Test	[SELECT FROM: Mechanisms for developing, implementing, and maintaining plan of action and milestones]	



```
<control class="SP800-53" id="ca-5">
  <title>Plan of Action and Milestones</title>
  <param id="ca-05_odp">
    <prop name="alt-identifier" value="ca-5_prm_1"/>
    <prop name="label" class="sp800-53a" value="CA-05_ODP"/>
    <label>frequency</label>
  </param>
  <part id="ca-5_obj" name="assessment-objective">
    <prop name="label" class="sp800-53a" value="CA-05"/>
    <part id="ca-5_obj.a" name="assessment-objective">
      <prop name="label" class="sp800-53a" value="CA-05a."/>
      <p>a plan of action and milestones for the system is developed to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system;</p>
    </part>
    <part id="ca-5_obj.b" name="assessment-objective">
      <prop name="label" class="sp800-53a" value="CA-05b."/>
      <p>existing plan of action and milestones are updated on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.</p>
      <insert type="param" id-ref="ca-05_odp"/>
    </part>
  </part>
  <part id="ca-5_asm-examine" name="assessment-method">
    <prop name="method" ns="http://csrc.nist.gov/ns/nmf" value="EXAMINE"/>
    <prop name="label" class="sp800-53a" value="CA-05-Examine"/>
    <part name="assessment-objects">
      <p>Assessment, authorization, and monitoring policy</p>
      <p>procedures addressing plan of action and milestones</p>
      <p>control assessment plan</p>
      <p>control assessment report</p>
      <p>control assessment evidence</p>
      <p>plan of action and milestones</p>
      <p>system security plan</p>
    </part>
  </part>
</control>
```



Future Revisions of NIST SP 800-53



The screenshot shows the NIST CSRC website interface. At the top is the NIST logo and 'Information Technology Laboratory' text. Below is a blue banner for the 'COMPUTER SECURITY RESOURCE CENTER' with the CSRC logo. A navigation bar includes 'PROJECTS', 'NIST RISK MANAGEMENT FRAMEWORK', and 'SP 800-53 CONTROLS'. The main content area is titled 'NIST Risk Management Framework RMF' with social media icons. Below this is 'SP 800-53 Public Comments: Submit and View' with links for 'Public Comment Home', 'More Information', 'User's Guide', and 'FAQ'. A table lists actions: 'New' (Suggest a new SP 800-53 control or control enhancement), 'Edit' (Suggest a change to an existing SP 800-53 control or control enhancement), 'Candidates' (View proposed changes to the SP 800-53 controls), and 'Awaiting' (View proposed changes awaiting release). A QR code is on the left, and a tracking number input field with a 'Find' button is on the right. A footer note states: 'This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.'

New	Suggest a new SP 800-53 control or control enhancement
Edit	Suggest a change to an existing SP 800-53 control or control enhancement
Candidates	View proposed changes to the SP 800-53 controls
Awaiting	View proposed changes awaiting release

View status of candidate and proposals awaiting release.

Tracking Number:

This site is protected by reCAPTCHA and the Google [Privacy Policy](#) and [Terms of Service](#) apply.



SP 800-53 controls, baselines, and assessment procedures* as a **machine-readable & web-based data set**



Suggest new controls, improve existing controls anytime.

Comment on draft controls and see feedback from others.



Receive status updates on your comments!



Preview planned changes in next revision.

<https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/public-comments>

Additional SP 800-53 Resources Available



SP 800-53 Release Search

SP 800-53 Rev 5.1 and SP 800-53B Latest

Versions

Security Controls

- [Low-Impact Security Baseline](#)
- [Moderate-Impact Security Baseline](#)
- [High-Impact Security Baseline](#)
- [Privacy Control Baseline](#)
- [All Controls](#)

Other Links

- [Control Families](#)
- [Search](#)
- [Downloads](#)

Other Revisions

- [SP 800-53 Rev 4.0](#)



SP 800-53 Downloads

Download the SP 800-53 Controls in Different Data Formats

SP 800-53, Revision 5 Controls CURRENT VERSION 5.1

- Download [XML](#) (controls and baselines)
- Download [PDF](#)
- Download [CSV](#)
- Download [Spreadsheet](#)
- Download [XSL Transform](#)
- [OSCAL GitHub](#)

Authoritative Source: [NIST SP 800-53, Revision 5](#)
(includes errata updates 12/2020)

SP 800-53A, Revision 5 Assessment Procedures

- Download [Plain Text](#)
- Download [CSV](#)
- Download [Spreadsheet](#)
- [OSCAL GitHub](#)

Authoritative Source: [NIST SP 800-53A, Revision 5](#)

SP 800-53B Control Baselines

CURRENT VERSION

- Download [XML](#) (controls and baselines)
- Download [PDF](#)
- Download CSV [\[Low\]](#) [\[Moderate\]](#) [\[High\]](#) [\[Privacy\]](#)
- Download All Control Baselines [Spreadsheet](#)

Authoritative Source: [NIST SP 800-53B](#)
(includes errata updates 12/2020)



OSCAL

Open Security Controls
Assessment Language




Bridging Two Communities...

**Systems
Security
Engineering**



**Risk
Management
Framework**



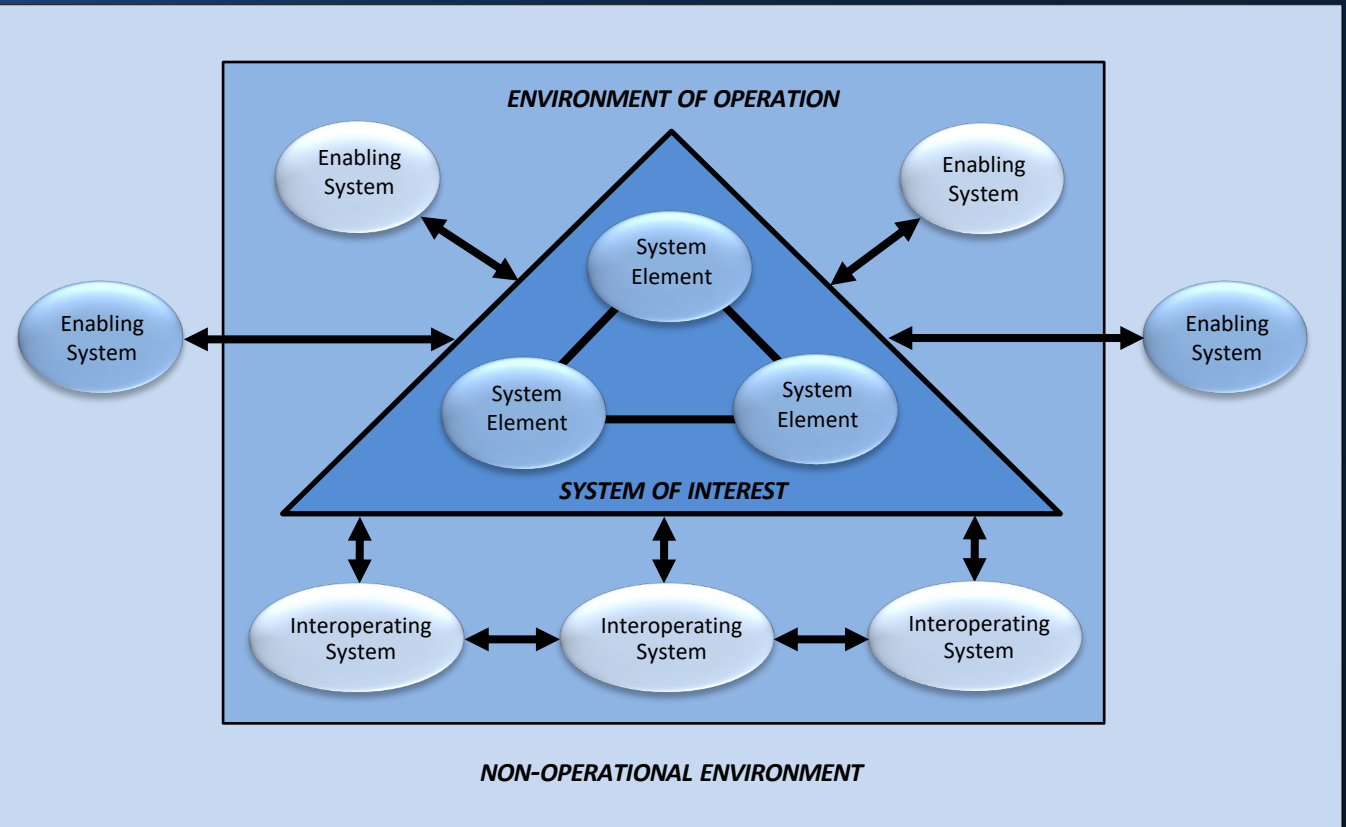
“Security is embedded in systems. Rather than two engineering groups designing two systems, one intended to protect the other, systems engineering specifies and designs a single system with security embedded in the system and its components.”

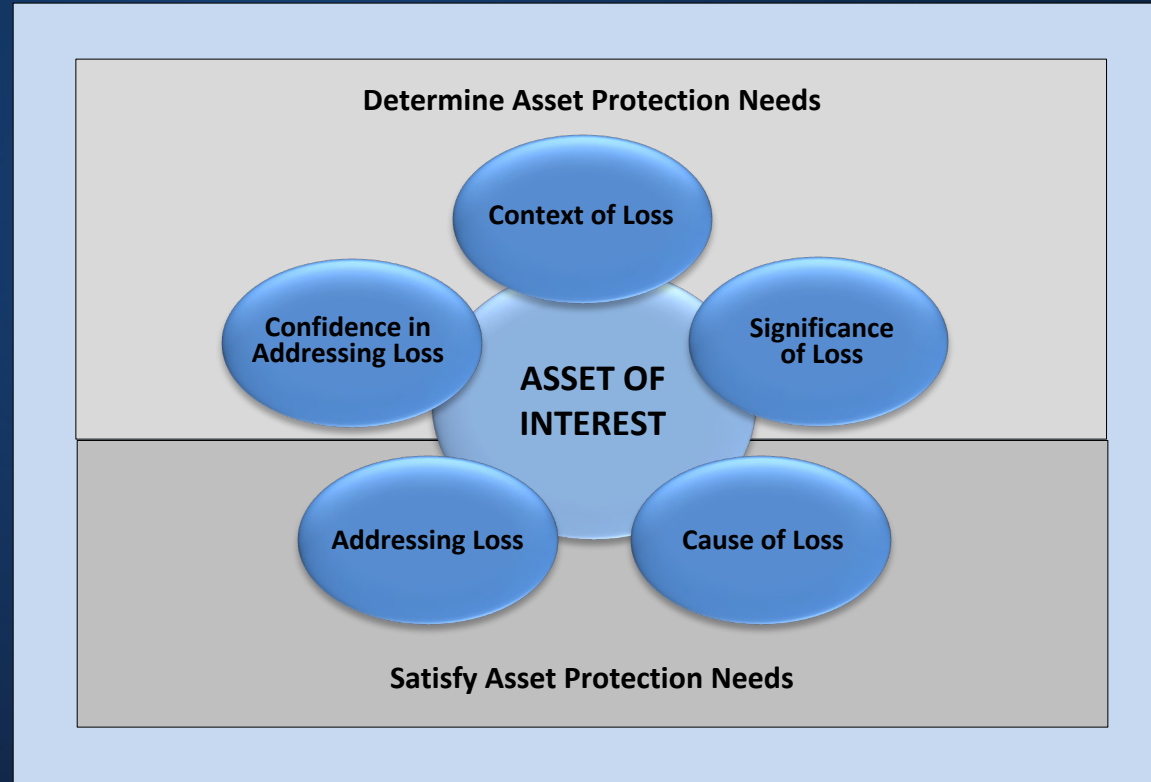
-- *Security in the Future of Systems Engineering (FuSE), a Roadmap of Foundational Concepts, 2021 INCOSE International Symposium*



Critical interdependencies and relationships among internal system elements, systems within enterprise environments, and systems in external environments that affect security solutions.

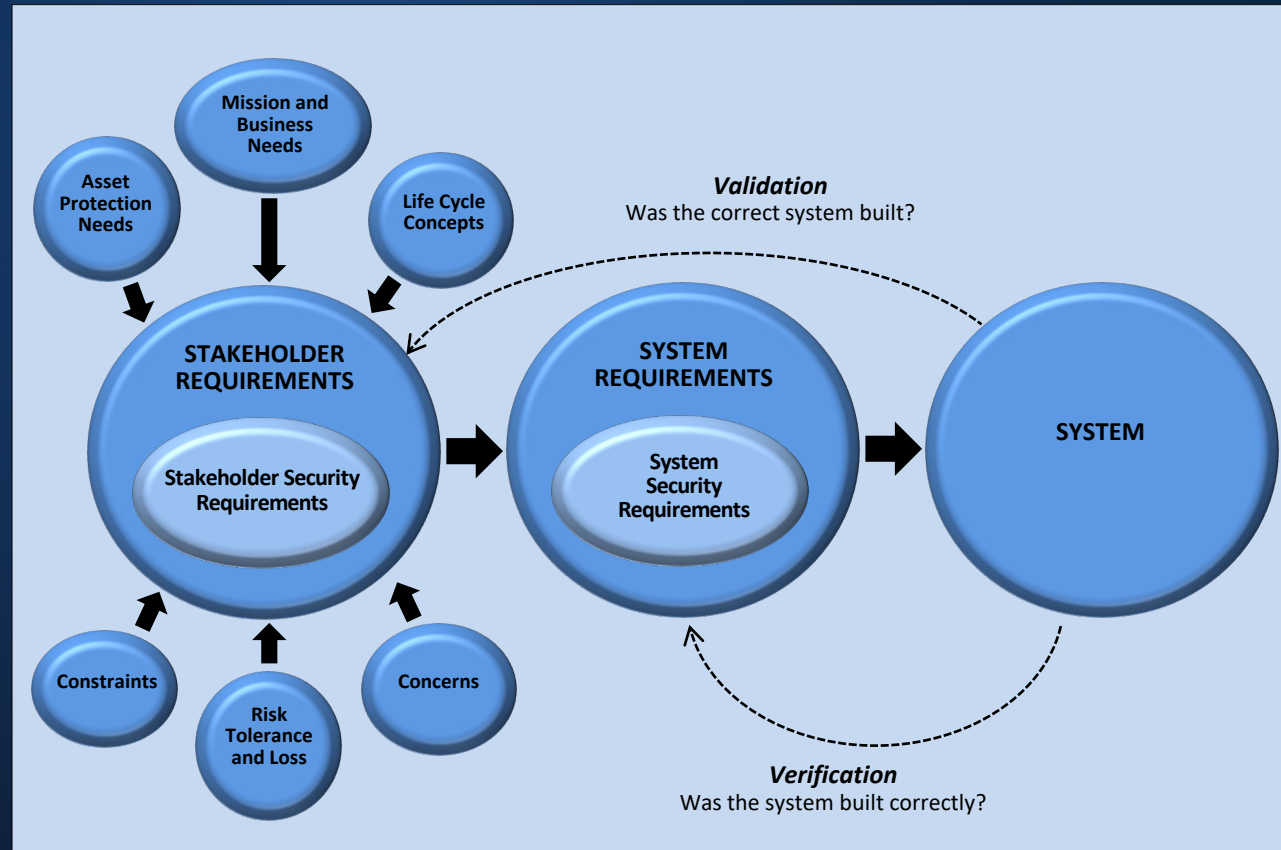
System of Systems





Security Engineering Focuses on Asset Loss

Requirements Engineering



Principles for Trustworthy Secure Design

Anomaly Detection	Least Privilege
Clear Abstractions	Least Sharing
Commensurate Protection	Loss Margins
Commensurate Response	Mediated Access
Commensurate Rigor	Minimize Detectability
Commensurate Trustworthiness	Minimal Trusted Elements
Compositional Trustworthiness	Protective Failure
Continuous Protection	Protective Recovery
Defense In Depth	Redundancy
Distributed Privilege	Protective Defaults
Diversity (Dynamicity)	Reduced Complexity
Domain Separation	Self-Reliant Trustworthiness
Hierarchical Protection	Structured Composition and Decomposition
Least Functionality	Substantiated Trustworthiness
Least Persistence	Trustworthy System Control

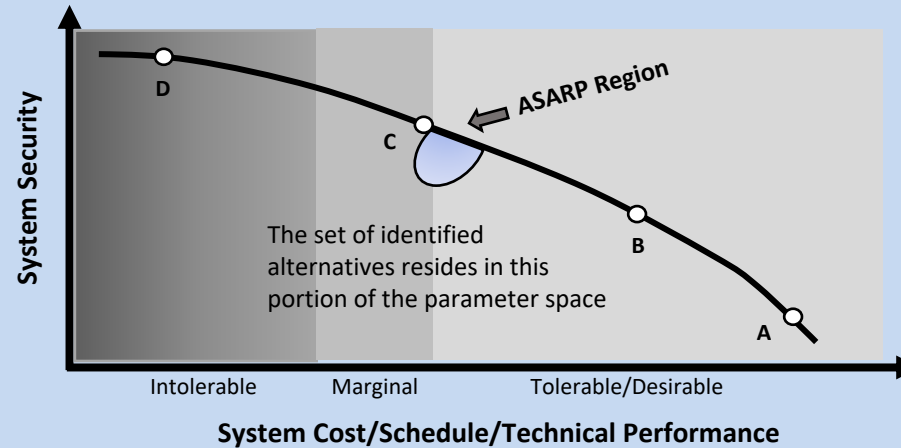
The Limits of Security

No system can provide *absolute* security due to the limits of human certainty, the uncertainty that exists in the life cycle of every system, and the constraints of cost, schedule, performance, feasibility, and practicality.

As such, trade-offs made routinely across contradictory, competing, and conflicting needs and constraints are optimized to achieve *adequate* security, which reflects a decision made by stakeholders.



Adequate Security



- A:** Large increases in system security can be achieved by addressing basic security issues. Little cost, schedule, or technical impact.
- B:** Basic security issues have been addressed but significant security can still be “bought” without failing to meet cost, schedule, or technical performance requirements.
- C:** Limit of ASARP regime has been reached but significant increases in security can be “bought” without exceeding tolerable limits of cost, schedule, or technical performance requirements.
- D:** Limit of achievable security has been met. Increased security cannot be “bought” at any cost.

Adapted from NASA.

As secure as reasonably practicable...

Assurance Case

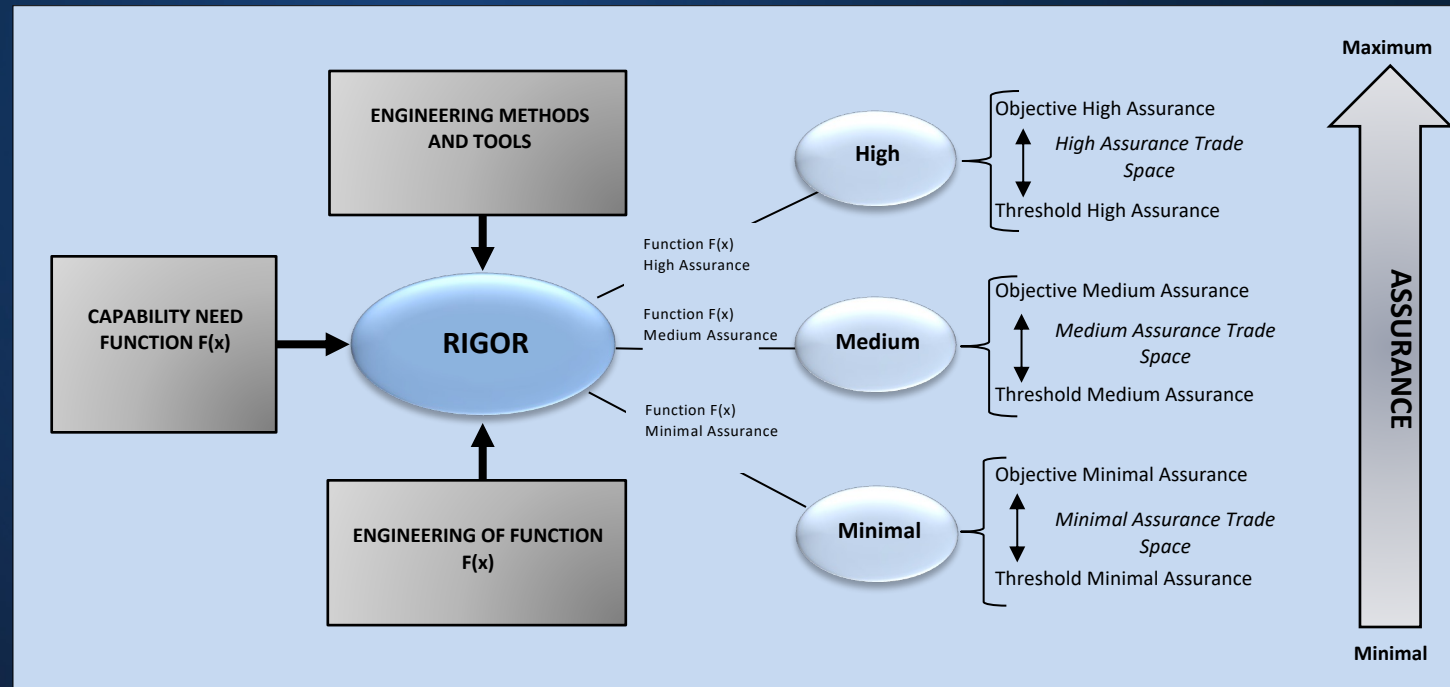
An *assurance case* is a reasoned, auditable artifact that is created to support the contention that a top-level claim is satisfied.

An assurance case contains:

- One or more claims about properties
- Arguments that logically link the evidence and any assumptions
 - A body of evidence
 - Justification of the choice of a top-level claim and the method of reasoning



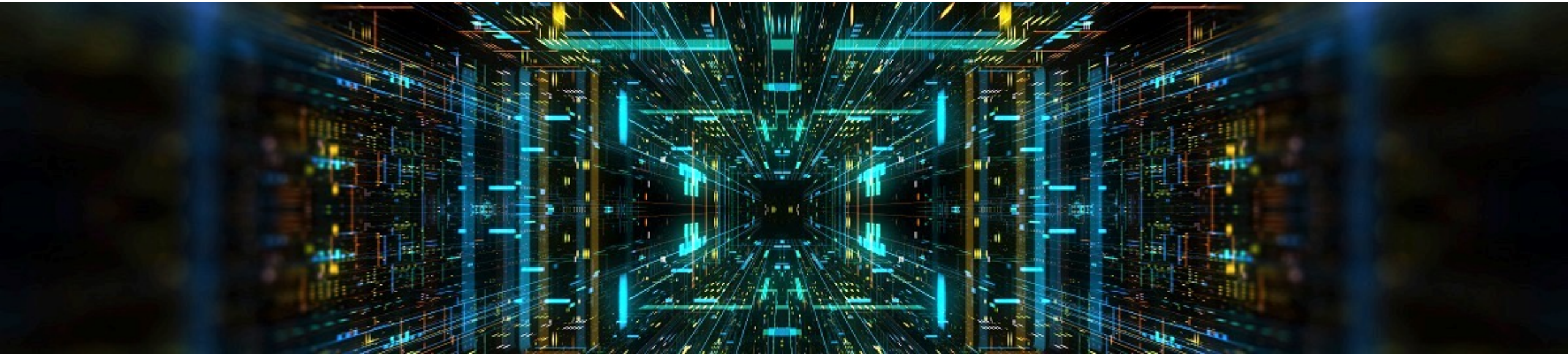
Assurance and Rigor



Key Issues for Building Trustworthy Secure Systems

Applied Research at the NCCoE

Post-Quantum Cryptography



Accelerating the migration to new cryptographic algorithms that are resistant to quantum computer-based attacks

Hardware Security of Trust



The foundation to any data center or edge computing security strategy should be securing the physical platform where workloads will be executed. The physical platform provides the initial protections to help ensure that higher-layer security controls can be trusted.

Secure Telecommunications – 5G



Cybersecurity guidance to help consumers and operators of 5G networks securely adopt this technology as the development, deployment, and usage of 5G simultaneously evolves

Zero Trust Architectures



Designing and deploying an end-to-end zero trust architecture(s) according to the concepts and tenets outlined in NIST SP 800-207, *Zero Trust Architecture*.



Ron Ross

Email: ron.ross@nist.gov

Mobile: (301) 651-5083

Web: <http://csrc.nist.gov>

Twitter: <https://twitter.com/ronrossecure>

LinkedIn: <https://www.linkedin.com/in/ronrossecure>