The NIST Security & Privacy Controls Catalog (SP 800-53): What's New and Looking Ahead

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

ISSA DC Chapter

September 15, 2020

Victoria Yan Pillitteri

victoria.yan@nist.gov

Agenda

- Evolution of NIST Special Publication (SP) 800-53
- Summary of Changes in NIST SP 800-53, Revision 5
  - Control Structure
  - Control Baselines and Supplemental Materials
  - Control Families and Controls
  - Privacy & Supply Chain Risk Management
- Next Steps: Publications
- Future Revisions of NIST SP 800-53
- Resources and Q&A

Evolution of NIST SP 800-53

Nov 2001
NIST SP 800-26, *Security Self-Assessment Guide for IT Systems,* published

Dec 2006
NIST SP 800-53, Rev. 1 published

Added industrial control systems guidance

Dec 2007
NIST SP 800-53, Rev. 2 published

Aug 2009
NIST SP 800-53, Rev. 3 published

Became Joint Task Force (JTF) Publication; added guidance on Information Security Programs (PM Family)

Dec 2014
NIST SP 800-53A, Rev. 4, published

2001 2005 2006 2007 2008 2009 2013 2014

Feb 2005
NIST SP 800-53, *Recommended Security Controls for Federal Information Systems,* originally published

17 security control families based on FIPS 200

July 2008
NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, published

April 2013
NIST SP 800-53, Rev. 4 published

Added Privacy Control Catalog (Appendix J)

Summary of Changes in SP 800-53, Rev 5

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

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

- 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) and Supply Chain Risk Management (SR)

Outcome-Focused Control Structure

SP 800-53, Revision 4

SC-10 NETWORK DISCONNECT

Control: The *information system* terminates the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.

SP 800-53, Revision 5

SC-10 NETWORK DISCONNECT

Control: Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time-period] of inactivity.

Appendix C, Control Summaries includes an *"implemented by"* (system/organization) column.

Control Baselines & Supplemental Materials

- Mappings, control keywords, and a collaboration template will be posted as spreadsheets under **SP 800-53 Supplemental Resources**
- Analysis of **changes** between Rev 4 and Rev 5
- **New** Security Control Overlay Repository launched
- Control Baselines, Overlay and Tailoring Guidance moved to **SP 800-53B**
- Controls in **Open Security Control Assessment Language (OSCAL)** available

Control Families and Controls

New Controls and Control Enhancements

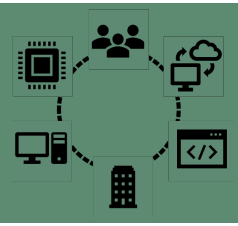
- New, state-of-the-practices controls
  - Systems security engineering
  - Cyber resiliency
  - Strengthen governance & accountability

Informed by threat intelligence & cyber-attack data

Privacy

- (Rev 4) Appendix J controls reorganized
- New PT control family
- Privacy integrated throughout
  - Additional discussion on collaboration
- New controls in PM family

Privacy integration into suite of RMF publications



Supply Chain

- New controls in PM family
- Supply chain risk management integrated throughout
- New SR control family

Alignment & integration of supply chain risk management

New Controls and Control Enhancements

SA-8 Security and Privacy Engineering Principles
SA-8 (1) Clear Abstractions
SA-8 (2) Least Common Mechanism
SA-8 (3) Modularity and Layering
SA-8 (4) Partially Ordered Dependencies
SA-8 (5) Efficiently Mediated Access
SA-8 (6) Minimized Sharing
…
SA-8 (33) Minimization

For example, these new control enhancements link to **security design principles** in **NIST SP 800-160, Volume 1**

New Controls and Control Enhancements

Rev4 Control Number	Rev4 Control Name	Rev5 Control Number	Rev5 Control Name	More than editorial or administrative change? (Y/N)	Changes	Change Details
AC-2(3)	Account Management | Disable Inactive Accounts	AC-2(3)	Disable Accounts	Y	Changes title Changes control text	Changes title from 'disable inactive' to 'disable' Control text enumerates conditions upon which to disable accounts, beyond those that are inactive
AC-2(4)	Account Management | Automated Audit Actions	AC-2(4)	Automated Audit Actions	Y	Changes control text Removes parameter Adds discussion	Removes parameter for notifying organization-defined personnel or roles
AC-2(5)	Account Management | Inactivity Logout	AC-2(5)	Inactivity Logout	N	Adds discussion	Minor
AC-2(6)	Account Management | Dynamic Privilege Management	AC-2(6)	Dynamic Privilege Management	N	Changes control text Changes discussion	Minor
AC-2(7)	Account Management | Role-Based Schemes	AC-2(7)	Privileged User Accounts	Y	Changes control text Adds parameter Removes parameter Changes discussion	New parameter requires the use of either role-based or attribute-based access scheme to establish and administer privileged user accounts New control text adds monitoring of attribute assignments Revised control text generalizes monitor changes to roles or attributes Removes parameter specifying organization-defined actions, replaces text with "revoke access"

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

Privacy: Appendix J Reorganization

SP 800-53, Rev 4 App J Control	SP 800-53, Rev 5 Families
AP-1	PT
AP-2	PT
AR-1	PM
AR-2	RA
AR-3	SA
AR-4	CA
AR-5	AT, PL
AR-6	PM
AR-7	PL, PM, PT, SI
AR-8	PM
DI-1	PM, SI
DI-2	PM, SI
DM-1	PM, PT, SC, SI

SP 800-53 Rev 4 App J Control	SP 800-53, Rev 5 Families
DM-2	MP, SI
DM-3	PM, SI
IP-1	PT
IP-2	AC, PM
IP-3	IR, PM, SI
IP-4	PM
SE-1	PM
SE-2	IR
TR-1	PM, PT, SC
TR-2	PT
TR-3	PM
UL-1	PT, SC
UL-2	AC, PT

Appendix J controls were moved and restructured for consistency

Privacy: New PT Control Family

PT Controls
PT-1 Policy and Procedures
PT-2 Authority to Process Personally Identifiable Information
PT-3 Personally Identifiable Information Processing Purposes
PT-4 Minimization
PT-5 Consent
PT-6 Privacy Notice
PT-7 System of Records Notice
PT-8 Specific Categories of Personally Identifiable Information
PT-9 Computer Matching Requirements

Rev 4

- Control Outcomes in Appendix J: Authority & Purpose (AP), Accountability, Audit & Risk Mgmt (AR), Data Integrity (DI)*, Data Minimization (DM), Individual Participation & Redress (IP) , Security (SE)*, Transparency (TR), Use Limitation (UL)

Rev 5
Initial Public Draft

- 2 Privacy control families: Individual Processing (IP) & Privacy Authorization (PA)

Rev 5
Final Public Draft/ Final

- 1 privacy control family: PII Processing and Transparency

Privacy: Integration throughout SP 800-53

RA-3 RISK ASSESSMENT

Control:

a. Conduct a risk assessment, including:

1. The likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and

2. **The likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;**

b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

c. Document risk assessment results in [*Selection: security and **privacy plans**; risk assessment report;* [*Assignment: organization-defined document*]];

d. Review risk assessment results [*Assignment: organization-defined frequency*];

e. Disseminate risk assessment results to [*Assignment: organization-defined personnel or roles*]; and

f. Update the risk assessment [*Assignment: organization-defined frequency*] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

Discussion: Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation. Risk assessments also consider risk from external parties, including contractors who… **Organizations may benefit from collaboration between information security and privacy programs in selecting and implementing this control.**

Previous security risk management-focused controls now include privacy and highlight security & privacy collaboration, as applicable.

Privacy: New PT Control Family

SP 800-53 Rev 4, App J

AP-2 PURPOSE SPECIFICATION

Control: The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.

SP 800-53 Rev 5

PT-3 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES

Control:

a. Identify and document the [Assignment: organization-defined purpose(s)] for processing personally identifiable information;

b. Describe the purpose(s) in the public privacy notices and policies of the organization;

c. Restrict the [*Assignment: organization-defined processing*] of personally identifiable information to only that which is compatible with the identified purpose(s); and

d. Monitor changes in processing personally identifiable information and implement [*Assignment: organization-defined mechanisms*] to ensure that any changes are made in accordance with [*Assignment: organization-defined requirements*].

Control Enhancements:

(1) PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES | DATA TAGGING

- ✓ Traceable to Rev 4, Appendix J
- ✓ Traceable to OMB Circular A-130

Privacy: Updates to PM Control Family

PM Control
PM-1 Information Security Program Plan
PM-2 Information Security Program Leadership Role
PM-3 Information Security and Privacy Resources
PM-4 Plan of Action and Milestones Process
PM-5 System Inventory
PM-6 Measures of Performance
PM-7 Enterprise Architecture
PM-8 Critical Infrastructure Plan
PM-9 Risk Management Strategy
PM-10 Authorization Process
PM-11 Mission and Business Process Definition
PM-12 Insider Threat Program
PM-13 Security and Privacy Workforce
PM-14 Testing, Training, and Monitoring
PM-15 Security and Privacy Groups and Associations
PM-16 Threat Awareness Program
PM-17 Protecting CUI on External Systems
PM-18 Privacy Program Plan
PM-19 Privacy Program Leadership Role
PM-20 Dissemination of Privacy Program Information
PM-21 Accounting of Disclosures
PM-22 Personally Identifiable Information Quality Management
PM-23 Data Governance Body
PM-24 Data Integrity Board
PM-25 Minimization of PII Used in Testing Training, and Research
PM-26 Complaint Management
PM-27 Privacy Reporting
PM-28 Risk Framing
PM-29 Risk Management Program Leadership Roles
PM-30 Supply Chain Risk Management Strategy
PM-31 Continuous Monitoring Strategy
PM-32 Purposing
PM-33 Privacy Policies on Websites, Applications, and Digital Services

✓ **New Privacy Program Management Controls**

✓ *Privacy integrated into applicable PM controls*

Supply Chain: Updates to PM Control Family

PM Control
PM-1 Information Security Program Plan
PM-2 Information Security Program Leadership Role
PM-3 Information Security and Privacy Resources
PM-4 Plan of Action and Milestones Process
PM-5 System Inventory
PM-6 Measures of Performance
PM-7 Enterprise Architecture
PM-8 Critical Infrastructure Plan
PM-9 Risk Management Strategy
PM-10 Authorization Process
PM-11 Mission and Business Process Definition
PM-12 Insider Threat Program
PM-13 Security and Privacy Workforce
PM-14 Testing, Training, and Monitoring
PM-15 Security and Privacy Groups and Associations
PM-16 Threat Awareness Program
PM-17 Protecting CUI on External Systems
PM-18 Privacy Program Plan
PM-19 Privacy Program Leadership Role
PM-20 Dissemination of Privacy Program Information
PM-21 Accounting of Disclosures
PM-22 Personally Identifiable Information Quality Management
PM-23 Data Governance Body
PM-24 Data Integrity Board
PM-25 Minimization of PII Used in Testing Training, and Research
PM-26 Complaint Management
PM-27 Privacy Reporting
PM-28 Risk Framing
PM-29 Risk Management Program Leadership Roles
PM-30 Supply Chain Risk Management Strategy
PM-31 Continuous Monitoring Strategy
PM-32 Purposing
PM-33 Privacy Policies on Websites, Applications, and Digital Services

- ✓ **New Supply Chain Risk Management Program Management Controls**
- ✓ *Supply Chain Risk Management integrated into applicable PM controls*

Supply Chain: Integration throughout SP 800-53

RA-3 RISK ASSESSMENT

…

Control Enhancements:

(1) RISK ASSESSMENT | SUPPLY CHAIN RISK ASSESSMENT

(a) Assess supply chain risks associated with [Assignment: organization-defined systems, system components, and system services]; and

(b) Update the supply chain risk assessment [Assignment: organization-defined frequency], when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

Discussion: Supply chain-related events include disruption, use of defective components, insertion of counterfeits, theft, malicious development practices, improper delivery practices, and insertion of malicious code. These events can have a significant impact on the confidentiality, integrity, or availability of a system and its information and, therefore, can also adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. The supply chain-related events may be unintentional or malicious and can occur at any point during the system life cycle. An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

Related Controls: RA-2, RA-9, PM-17, PM-30, SR-2.

Previous security risk management-focused controls now include supply chain integrated in control or highlighted in the discussion.

Supply Chain: New SR Control Family

SR Controls
SR-1 Policy and Procedures
SR-2 Supply Chain Risk Management
SR-3 Supply Chain Controls and Processes
SR-4 Provenance
SR-5 Acquisition Strategies, Tools, and Methods
SR-6 Supplier Assessments and Reviews
SR-7 Supply Chain Operations Security
SR-8 Notification Agreements
SR-9 Tamper Resistance and Detection
SR-10 Inspection of Systems or Components
SR-11 Component Authenticity
SR-12 Component Disposal

Rev 4

- Addressed in SA Control Family

Rev 5
Initial Public Draft

- Addressed in SA Control Family

Rev 5
Final Public Draft/ Final

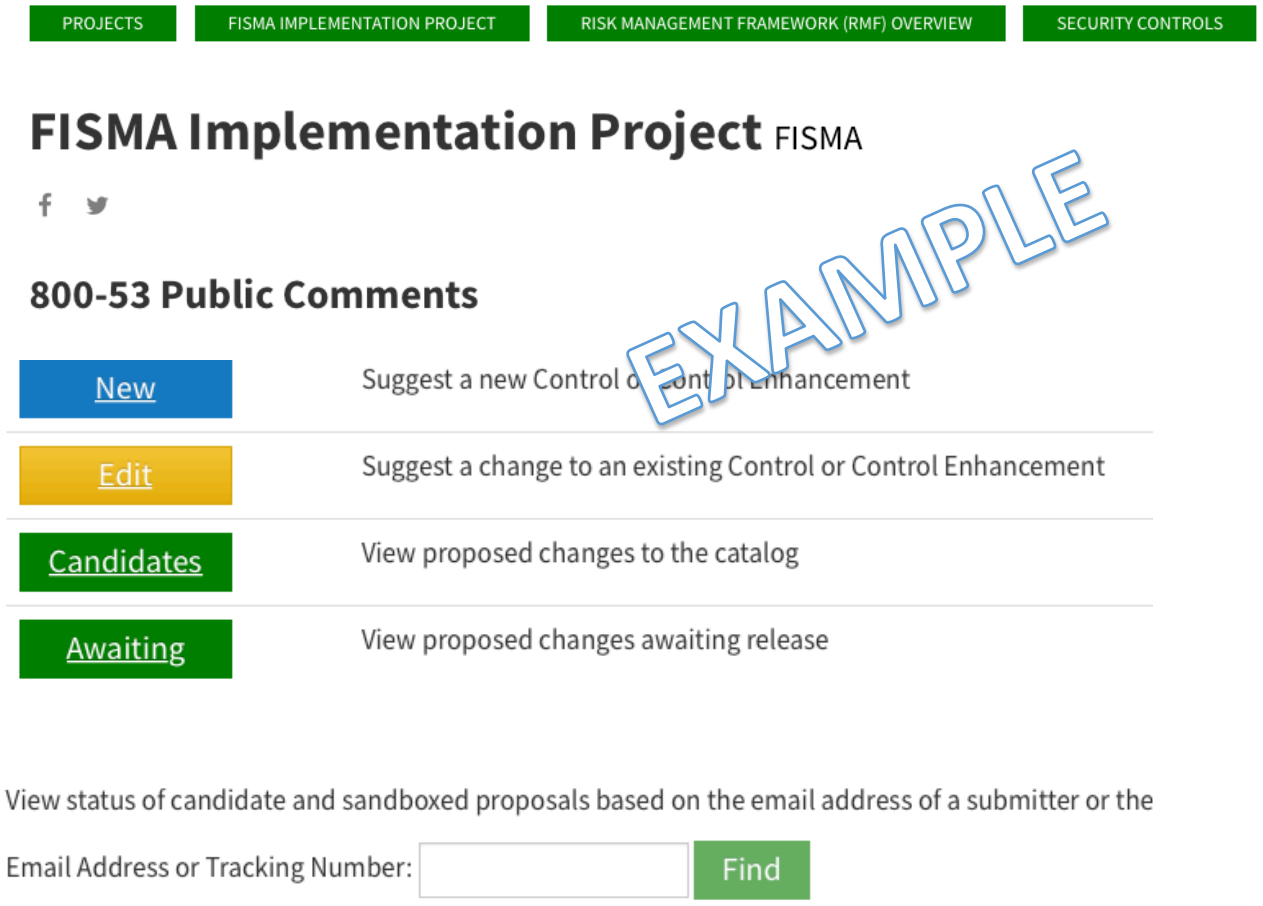
- Addressed throughout, in PM Control Family, and SR Control Family

Next Steps: Publications

1. Publish NIST SP 800-53, Revision 5 (Final) & supplemental resources

- Adjudicate comments on Draft NIST SP 800-53B
- Continue to develop NIST SP 800-53A, Revision 5
- Continue to develop Draft NIST SP 800-161, Revision 1
- Identify and update other publications supporting the NIST Risk Management Framework (SP 800-37)

Future Revisions of NIST SP 800-53



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

Quarterly **minor updates***
(or more frequent than current errata)

Annual **major updates***
(or more frequent than new revisions)

Ongoing public comment and review

Dynamically generate and download a MS Word or PDF file

Additional Resources

Risk Management Framework

https://nist.gov/RMF

Program overview & links to additional resources, including Quick Start Guides, an updated online training* on SP 800-37, Revision 2, and the Security Control Overlay Repository

DRAFT SP 800-53, Revision 5

https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft

Final public draft, summary of significant changes from Rev 4 and analysis spreadsheet, controls in .xls format, FAQ

OSCAL on GitHub

https://github.com/usnistgov/oscal-content

OSCAL content for SP 800-53 controls (Rev 4, 5, and draft baselines).

Available in XML, JSON, and YAML

SP 800-53, Revision 4 Controls

https://nvd.nist.gov/800-53

Search web-based controls, downloads of SP 800-53 and SP 800-53A in alternative formats (XML, tab-delimited, CSV)

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

STAY IN TOUCH

CONTACT US

nist.gov/RMF

sec-cert@nist.gov

@NISTcyber