What’s New in Draft NIST Special Publication 800-53, Revision 5

Security and Privacy Controls for Information Systems and Organizations

Virtual Event

April 8, 2020

2:00 – 3:30 PM ET

Virtual Event Resources and FAQ

This virtual event will be recorded and available by April 17th, 2020;
slides from today's event are currently available: https://go.usa.gov/xd7Vq

Technical Issues

For technical issues using slido, connection, sound, video, etc., **please first refer to the troubleshooting steps** listed on the Event page.

If the technical issues have not been resolved **after trying the troubleshooting steps**, please contact: webcast@nist.gov

Questions for the Speakers*

Please check the NIST SP 800-53 Rev. 5 (final public draft) FAQ Page: https://go.usa.gov/xvxtq

OR

Submit questions at any time during the presentation using the slido website or app.

*Speakers may not be able to respond to each question submitted during the Q&A; an updated FAQ will be posted that addresses submitted questions with no attribution

Agenda: What's New in Draft NIST SP 800-53, Revision 5

Security and Privacy Controls for Information Systems and Organizations

2:00 PM ET	Welcome and Opening Remarks	Ron Ross, NIST Fellow and Joint Task Force Working Group Leader
2:20 PM ET	What's New in the NIST SP 800-53, Revision 5 (Final Public Draft)	Victoria Yan Pillitteri Naomi Lefkovitz Jon Boyens
2:50 PM ET	Feedback Requested: Security and Privacy Collaboration Index	Naomi Lefkovitz
2:55 PM ET	Next Steps, Resources and Contact	Victoria Yan Pillitteri
3:00 PM ET	Live Q&A Chat Join the discussion through the slido "ask the speaker" feature!	Speakers may not be able to respond to each question submitted during the Q&A; an updated FAQ will be posted that addresses submitted questions

Agenda: What’s New in Draft NIST SP 800-53, Revision 5

Security and Privacy Controls for Information Systems and Organizations

2:00 PM ET	**Welcome and Opening Remarks**	**Ron Ross, NIST Fellow and Joint Task Force Working Group Leader**
2:20 PM ET	What’s New in the NIST SP 800-53, Revision 5 (Final Public Draft)	Victoria Yan Pillitteri Naomi Lefkovitz Jon Boyens
2:50 PM ET	Feedback Requested: Security and Privacy Collaboration Index	Naomi Lefkovitz
2:55 PM ET	Next Steps, Resources and Contact	Victoria Yan Pillitteri
3:00 PM ET	Live Q&A Chat Join the discussion through the slido “ask the speaker” feature!	Speakers may not be able to respond to each question submitted during the Q&A; an updated FAQ will be posted that addresses submitted questions

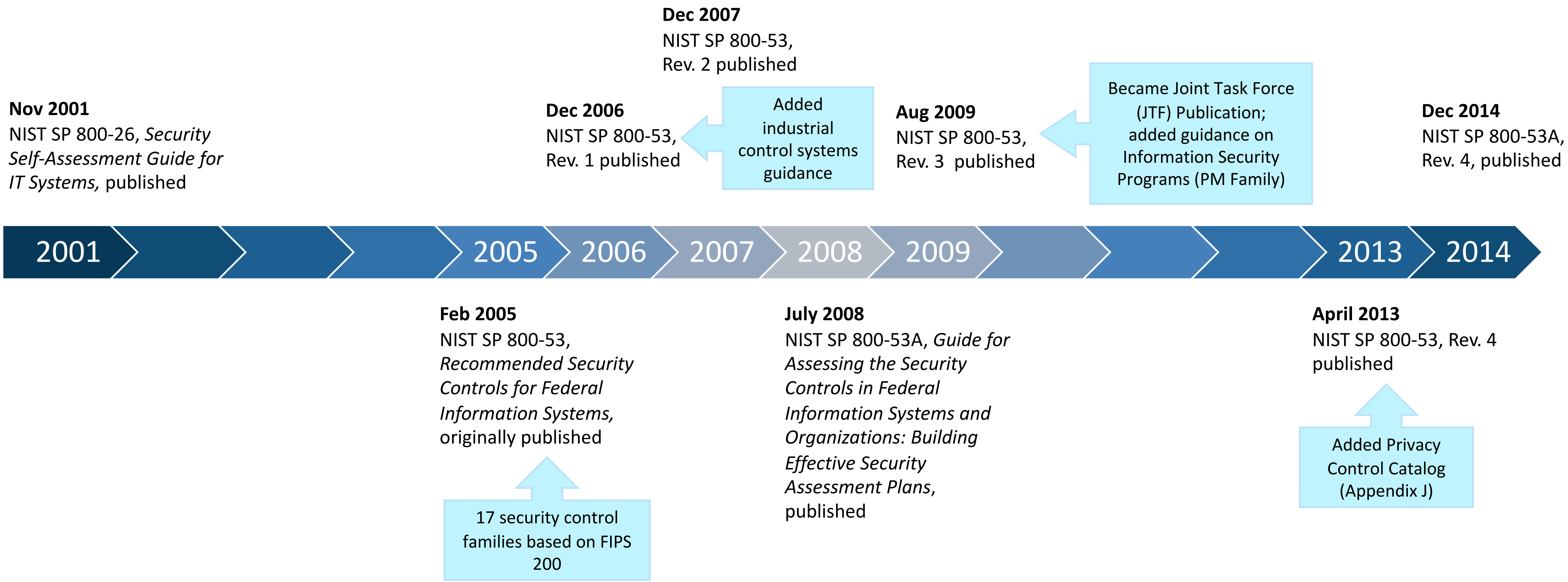
NIST SP 800-53, Revision 5

Next Generation Controls for Systems and Organizations

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

NIST SP 800-53 Revision 5 (FPD) FAQ: https://go.usa.gov/xvxtq
Still have questions? Email sec-cert@nist.gov

Background: NIST Special Publication (SP) 800-53



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

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

17 security control families based on FIPS 200

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

Added industrial control systems guidance

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

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

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

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

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

Added Privacy Control Catalog (Appendix J)

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

Agenda: What’s New in Draft NIST SP 800-53, Revision 5

Security and Privacy Controls for Information Systems and Organizations

2:00 PM ET	Welcome and Opening Remarks	Ron Ross, NIST Fellow and Joint Task Force Working Group Leader
2:20 PM ET	**What’s New in the NIST SP 800-53, Revision 5 (Final Public Draft)**	**Victoria Yan Pillitteri** **Naomi Lefkovitz** **Jon Boyens**
2:50 PM ET	Feedback Requested: Security and Privacy Collaboration Index	Naomi Lefkovitz
2:55 PM ET	Next Steps, Resources and Contact	Victoria Yan Pillitteri
3:00 PM ET	Live Q&A Chat Join the discussion through the slido “ask the speaker” feature!	Speakers may not be able to respond to each question submitted during the Q&A; an updated FAQ will be posted that addresses submitted questions

Summary of Significant Changes in NIST SP 800-53

SP 800-53, Rev. 4	SP 800-53, Rev. 5 (Final Public Draft)
	Control structure updated to be more outcome-focused
	New controls, control enhancements, and discussion to address evolving threat landscape (including IPv6 transition)
	Control baselines (security & privacy), overlay and tailoring guidance moved to *forthcoming* draft SP 800-53B
	Mappings to ISO 27001 and 15408 moved; new CSF mapping; new PF mapping will be posted online *when Rev 5 finalized*
	Privacy and supply chain risk management controls added to Program Management (PM) Family
Appendix J – Privacy Control Catalog (8 families: AP – Authority & Purpose; AR – Accountability, Audit, & Risk Management; DI - Data Quality & Integrity; DM – Data Minimization & Retention; IP – Individual Participation and Redress; SE – Security; TR – Transparency; UL – Use Limitation)	• Privacy Control Family (PT – Personally Identifiable Information Processing and Transparency) • All other privacy controls integrated in other families, including Program Management
	New Supply Chain Risk Management (SR) Family

NIST SP 800-53 Revision 5 (FPD) FAQ: https://go.usa.gov/xvxtq
Still have questions? Email sec-cert@nist.gov

New Outcome-Focused Control Structure Example

SP 800-53 Rev 4

SC-10 NETWORK DISCONNECT

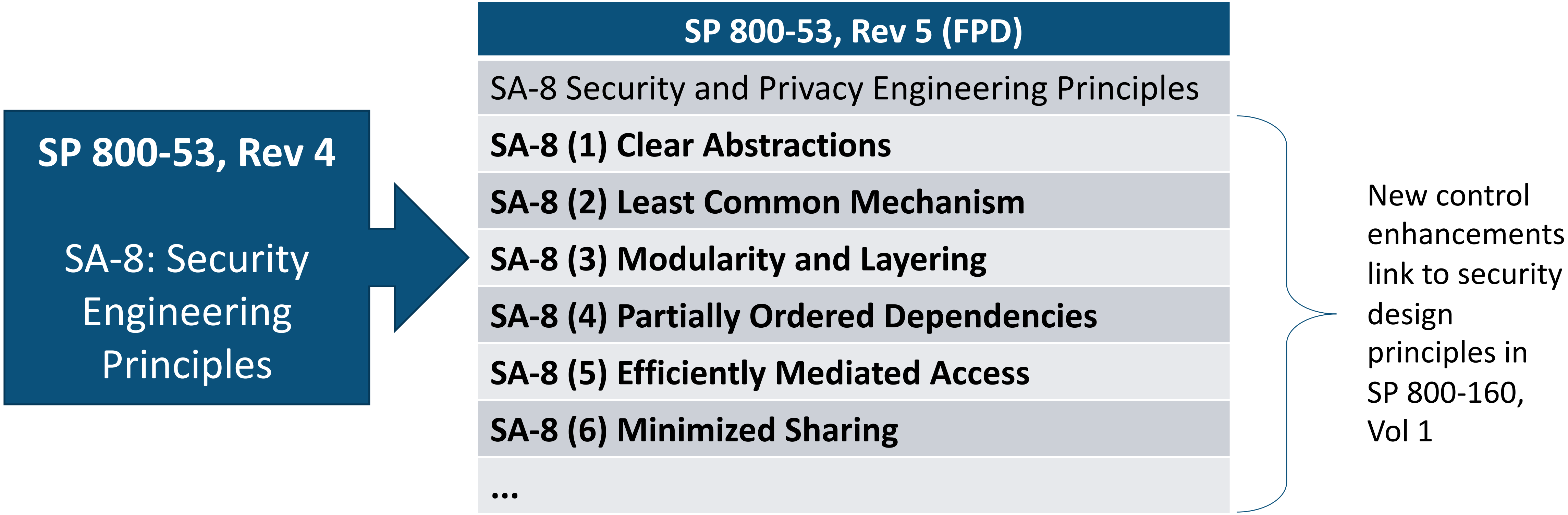
Control: The information system terminates the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.

SP 800-53 Rev 5 (FPD)

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.

New Systems Security Engineering Control Enhancements



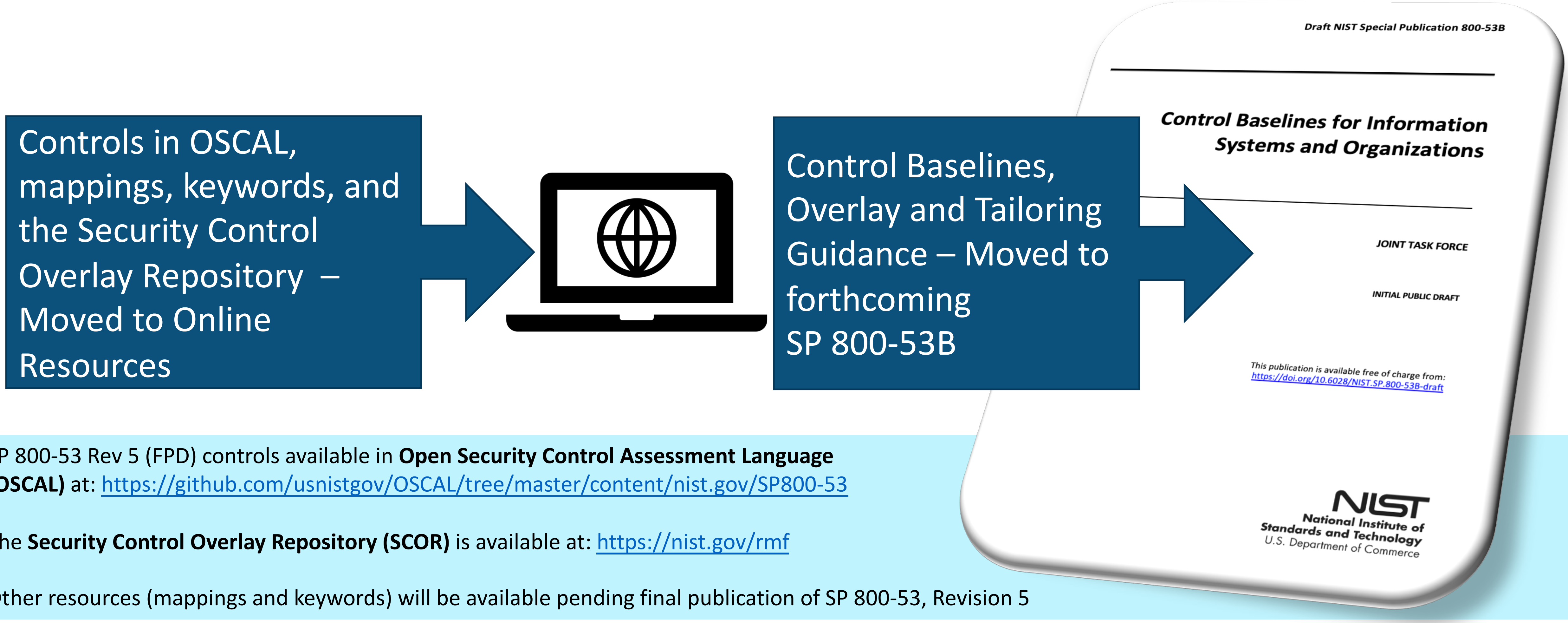
SP 800-53, Rev 4

SA-8: Security Engineering Principles

SP 800-53, Rev 5 (FPD)
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
…

New control enhancements link to security design principles in SP 800-160, Vol 1

Forthcoming: New Related Publication and Supplemental Materials Online



Controls in OSCAL, mappings, keywords, and the Security Control Overlay Repository – Moved to Online Resources

Control Baselines, Overlay and Tailoring Guidance – Moved to forthcoming SP 800-53B

Draft NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

INITIAL PUBLIC DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53B-draft

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

SP 800-53 Rev 5 (FPD) controls available in **Open Security Control Assessment Language (OSCAL)** at: https://github.com/usnistgov/OSCAL/tree/master/content/nist.gov/SP800-53

The **Security Control Overlay Repository (SCOR)** is available at: https://nist.gov/rmf

Other resources (mappings and keywords) will be available pending final publication of SP 800-53, Revision 5

Proposed Appendix J Reorganization

SP 800-53, Rev 4 App J Control	SP 800-53, Rev 5 Families	SP 800-53 Rev 4 App J Control	SP 800-53, Rev 5 Families
AP-1	PT	**DM-2**	MP, SI
AP-2	PT	**DM-3**	PM, SI
AR-1	PM	**IP-1**	PT
AR-2	RA	**IP-2**	AC, PM
AR-3	SA	**IP-3**	IR, PM, SI
AR-4	CA	**IP-4**	PM
AR-5	AT, PL	**SE-1**	PM
AR-6	PM	**SE-2**	IR
AR-7	PL, PM, PT, SI	**TR-1**	PM, PT, SC
AR-8	PM	**TR-2**	PT
DI-1	PM, SI	**TR-3**	PM
DI-2	PM, SI	**UL-1**	PT, SC
DM-1	PM, PT, SC, SI	**UL-2**	AC, PT

Proposed Program Management (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 Control
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

Proposed New Control Family: PII Processing and Transparency (PT)

PT Control
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

Risk Assessment Family: Security and Privacy Integration Example

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.

PII Processing and Transparency Family: Example

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 (FPD)

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

Attach data tags containing the following purposes to [*Assignment: organization-defined elements of personally identifiable information*]: [*Assignment: organization-defined processing purposes*].

(2) PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES | AUTOMATION

Track processing purposes of personally identifiable information using [*Assignment: organization-defined automated mechanisms*]

Supply Chain Risk Management (SCRM) Changes in Draft SP 800-53, Revision 5

- Align Supply Chain Risk Management with SP 800-161, CNSSD 505 & Further Consolidated Appropriations Act 2020, §208.
- Integrated SP 800-161 new controls/enhancements and Implementation Guidance into draft SP 800-53 Rev. 5.
- RA-3(1), Supply Chain Risk Assessment – new control enhancement.
- RA-9, Criticality Analysis - moved from SA-14, reference NISTIR 8179.
- PM-30, Program Management - to reflect a Tier 1 SCRM Plan/SCRM Strategy.
- Integrated NISTIR 8179, Criticality Analysis Process Model, throughout References.
- Last, but not least…………

Proposed New Control Family: Supply Chain Risk Management (SR)

SP 800-53, Rev 5 (FPD) SR Control		
SR-1 Policy and Procedures		**New**
SR-2 Supply Chain Risk Management		**New**
SR-3 Supply Chain Controls and Processes	*[SP 800-53, Rev 4, SA-12(15)]*	
SR-4 Provenance		**New**
SR-5 Acquisition Strategies, Tools, and Methods	*[SP 800-53, Rev 4, SA-12(1)]*	
SR-6 Supplier Reviews	*[SP 800-53, Rev 4, SA-12(2)]*	
SR-7 Supply Chain Operations Security	*[SP 800-53, Rev 4, SA-12(9)]*	
SR-8 Notification Agreements	*[SP 800-53, Rev 4, SA-12(12)]*	
SR-9 Tamper Resistance and Detection	*[SP 800-53, Rev 4, SA-18]*	
SR-10 Inspection of Systems or Components	*[SP 800-53, Rev 4, SA-18(2)]*	
SR-11 Component Authenticity	*[SP 800-53, Rev 4, SA-19]*	

Agenda: What's New in Draft NIST SP 800-53, Revision 5

Security and Privacy Controls for Information Systems and Organizations

2:00 PM ET	Welcome and Opening Remarks	Ron Ross, NIST Fellow and Joint Task Force Working Group Leader
2:20 PM ET	What's New in the NIST SP 800-53, Revision 5 (Final Public Draft)	Victoria Yan Pillitteri Naomi Lefkovitz Jon Boyens
2:50 PM ET	**Feedback Requested: Security and Privacy Collaboration Index**	**Naomi Lefkovitz**
2:55 PM ET	Next Steps, Resources and Contact	Victoria Yan Pillitteri
3:00 PM ET	Live Q&A Chat Join the discussion through the slido "ask the speaker" feature!	Speakers may not be able to respond to each question submitted during the Q&A; an updated FAQ will be posted that addresses submitted questions

Feedback Requested: Security and Privacy Collaboration Index

Purpose:
Provide better guidance on control implementation collaboration between security and privacy programs

NIST seeks feedback on the notional example included in the *Notes to Reviewers Supplement*

Three control families included as notional examples
Access Control (AC), Program Management (PM) and PII Processing and Transparency (PT)

Option 1		Option 2	
S	Controls are primarily implemented by security programs – minimal collaboration needed between security and privacy programs.	**S**	Security programs have primary responsibility for implementation – minimal collaboration needed between security and privacy programs.
S_P	Controls are generally implemented by security programs – moderate collaboration needed between security and privacy programs.		
SP	Controls are implemented by security and privacy programs – full collaboration needed between security and privacy programs.	**SP**	Security and privacy programs both have responsibilities for implementation – more than minimal collaboration is needed between security and privacy programs.
P_S	Controls are generally implemented by privacy programs – moderate collaboration needed between security and privacy programs.	**P**	Privacy programs have primary responsibility for implementation – minimal collaboration needed between security and privacy programs.
P	Controls are primarily implemented by privacy programs – minimal collaboration needed between security and privacy programs.		

Collaboration Index: Notional Examples

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX 3-GRADIENT SCALE	COLLABORATION INDEX 5-GRADIENT SCALE
ACCESS CONTROL (AC) FAMILY			
AC-1	**Policy and Procedures**	SP	SP
AC-2	**Account Management**	SP	S_P
AC-2(1)	AUTOMATED SYSTEM ACCOUNT MANAGEMENT	S	S
AC-2(2)	AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT	S	S
PROGRAM MANAGEMENT (PM) FAMILY			
PM-22	**Personally Identifiable Information Quality Management**	P	P
PM-23	**Data Governance Body**	SP	SP
PM-24	**Data Integrity Board**	P	P
PM-25	**Minimization of PII Used in Testing Training, and Research**	SP	SP
PM-26	**Complaint Management**	P	P
PERSONALLY IDENTIFIABLE INFORMATION PROCESSING & TRANSPARENCY (PT) FAMILY			
PT-1	**Policy and Procedures**	P	P
PT-2	**Authority to Process Personally Identifiable Information**	P	P
PT-2(1)	DATA TAGGING	SP	SP
PT-2(2)	AUTOMATION	SP	SP

Agenda: What's New in Draft NIST SP 800-53, Revision 5

Security and Privacy Controls for Information Systems and Organizations

2:00 PM ET	Welcome and Opening Remarks	Ron Ross, NIST Fellow and Joint Task Force Working Group Leader
2:20 PM ET	What's New in the NIST SP 800-53, Revision 5 (Final Public Draft)	Victoria Yan Pillitteri Naomi Lefkovitz Jon Boyens
2:50 PM ET	Feedback Requested: Security and Privacy Collaboration Index	Naomi Lefkovitz
2:55 PM ET	**Next Steps, Resources and Contact**	**Victoria Yan Pillitteri**
3:00 PM ET	Live Q&A Chat Join the discussion through the slido "ask the speaker" feature!	Speakers may not be able to respond to each question submitted during the Q&A; an updated FAQ will be posted that addresses submitted questions

Next Steps, Resources and Contact

NIST seeks your feedback on Draft SP 800-53, Rev. 5

https://go.usa.gov/xdevJ

- Draft SP 800-53, Rev 5
- Summary of Changes from Rev. 4
- Comment Template
- Open Security Control Assessment Language (XML, JSON, YAML) and .XLSX versions of controls

Public comment period: March 16 – May 15, 2020

Submit comments and questions to: sec-cert@nist.gov

A special note of appreciation to the team from NIST Conference Services and Computer Security Division – ***Hoyt Cox, Akeem Henry, Kevin Hill, Joe Hynes, Eduardo Takamura, Pauline Truong & Crissy Robinson*** – for coordinating this event! Thank you for job well done!!

LIVE CHAT Q&A

NIST Special Publication

800-53 Revision 5

Final Public Draft

Dr. Ron Ross

Introduction

Victoria Pillitteri

Security

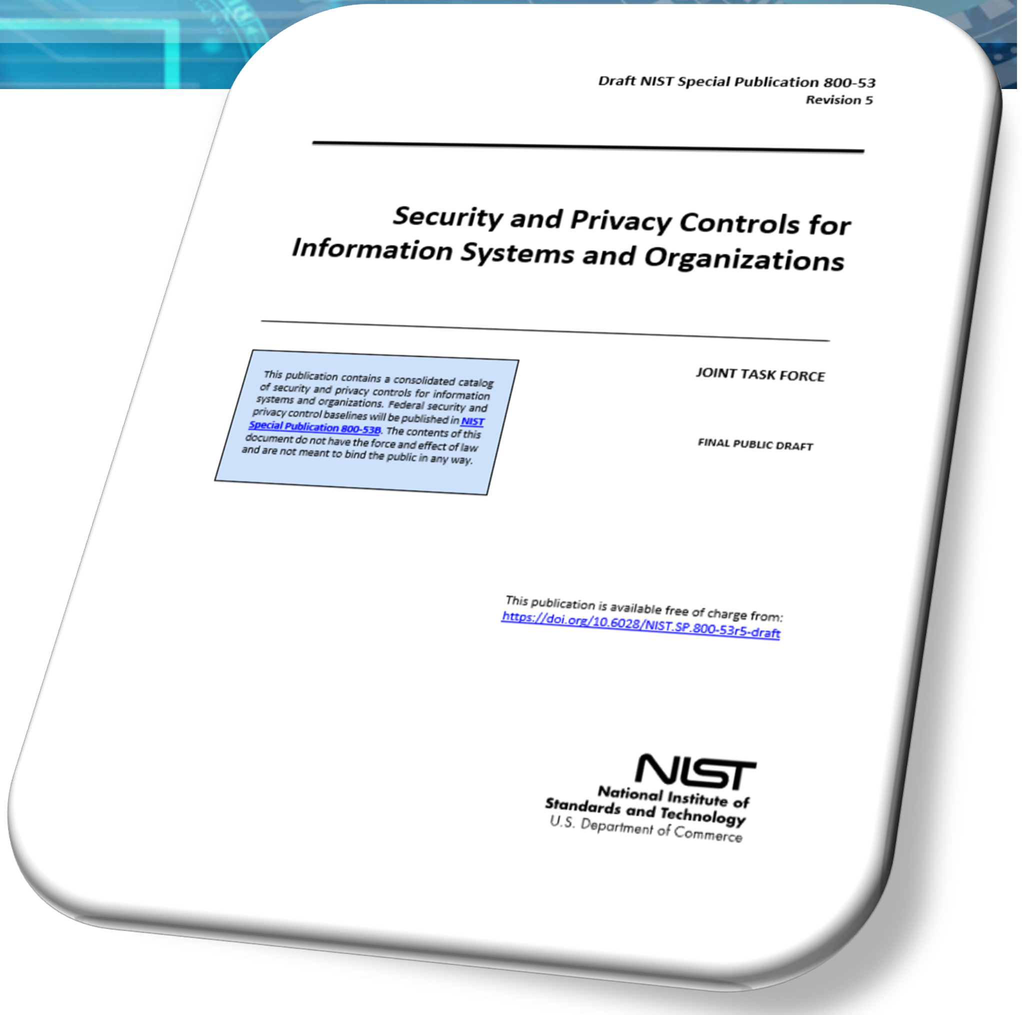
Naomi Lefkovitz

Privacy

Jon Boyens

Supply Chain

*Speakers may not be able to respond individually to each question submitted during the live chat Q&A; an updated FAQ will be posted that addresses submitted questions with no attribution. Questions can be submitted at any time to sec-cert@nist.gov



Draft NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

This publication contains a consolidated catalog of security and privacy controls for information systems and organizations. Federal security and privacy control baselines will be published in NIST Special Publication 800-53B. The contents of this document do not have the force and effect of law and are not meant to bind the public in any way.

JOINT TASK FORCE

FINAL PUBLIC DRAFT

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5-draft

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