Update on Draft Special Publication 800-53, Rev. 5

Information Security and Privacy Advisory Board

October 25, 2017

Naomi Lefkovitz, Applied Cybersecurity Division

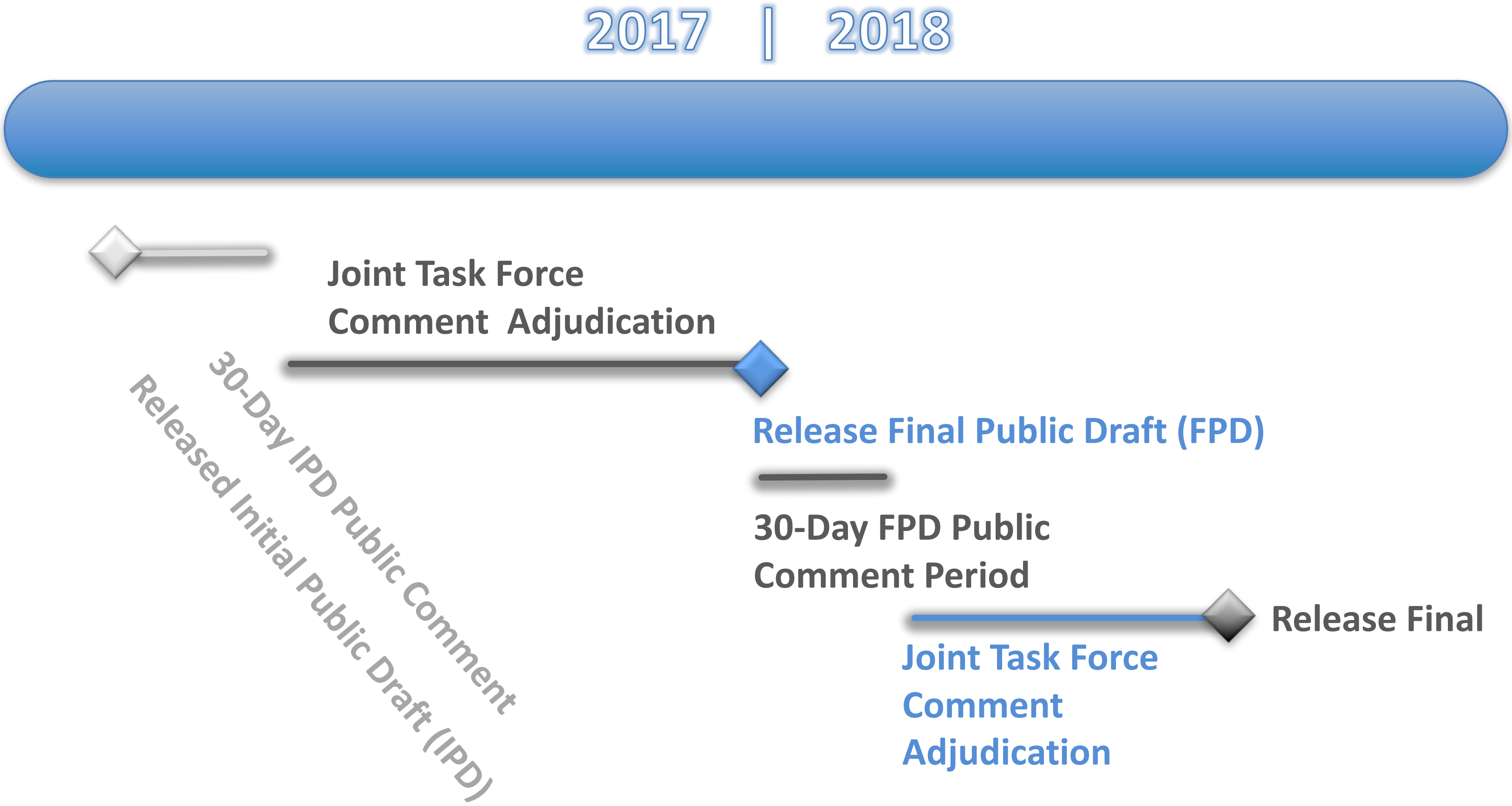
Vicky Yan Pillitteri, Computer Security Division

NIST
U.S. Department of Commerce

Overview

- Planned SP 800-53, Rev. 5 Publication Schedule
- Summary of Updates
- Stakeholder Engagement Prior to Initial Public Draft
- Public Comments Received (Initial Public Draft)
- Initial Comment Analysis
- Initial Public Draft Comment Adjudication
- Next Steps
- Update on Draft SP 800-37, Rev. 2
- Open Discussion

Planned SP 800-53, Rev. 5 Publication Schedule*



2017 | 2018

Released Initial Public Draft (IPD)

30-Day IPD Public Comment

Joint Task Force Comment Adjudication

Release Final Public Draft (FPD)

30-Day FPD Public Comment Period

Joint Task Force Comment Adjudication

Release Final

**Awaiting OMB Approval; Dates subject to change*

Summary of Updates

Major Changes between Rev. 4 and Draft Rev. 5

- Control structure updated to be more **outcome-based**;
- Full **integration of privacy controls and security controls** into one control catalog;
- Control **selection process separated** from controls;
- Integration with different risk management and cybersecurity approaches and lexicons, including the **Cybersecurity Framework**;
- Incorporating new, state-of-the-practice controls based on threat intelligence and empirical attack data, including **controls to strengthen cybersecurity and privacy governance and accountability**.

Stakeholder Engagement Prior to Initial Public Draft

Pre-Draft Call for Comments

- Call for pre-comments Feb 2016
- Received 750+ comments
- ~200 additional comments
- Adjudicated comments and made changes to inform the initial public draft
- Coordinated with SME teams (Privacy, Supply Chain Risk Mgmt, Identity Mgmt, Cryptography, etc.)

RMF Interagency Working Group

- OMB coordinated w/ CIO and CISO Council for agency representation; NIST led technical discussion
- Over 20 agencies participated
- Convened in July-Aug 2017
- Review SP 800-53 control baselines and SP 800-37
  - 175+ comments on 800-53
  - Strategic feedback on 800-37

Stakeholder Engagement Prior to Initial Public Draft (Cont.)

Privacy Coordination with the Federal Privacy Community

- Privacy Controls Workshop: Next Steps for NIST Special Publication 800-53, Appendix J (9/18/16)
- 800-53 privacy controls drafting process
  - Weekly: interagency core drafting team
  - Bimonthly: NIST FISMA team
  - Monthly: Federal Privacy Council Risk Management Subcommittee
- Coordination with OIRA Privacy Branch

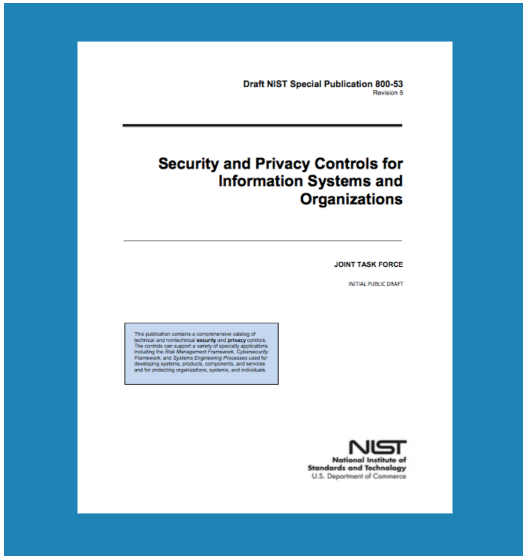
Public Comments Received (Initial Public Draft)

- Initial Public Draft (IPD) published Aug 15, 2017

- 30 day public comment period (through Sept 12, 2017)
  - Also published "red-line" version of controls and baselines that highlight ***significant technical updates and changes***

3000+ ***public comments***

115+ ***stakeholders***



Draft NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

INITIAL PUBLIC DRAFT

This publication contains a comprehensive catalog of technical and nontechnical **security** and **privacy** controls. The controls can support a variety of specialty applications including the *Risk Management Framework*, *Cybersecurity Framework*, and *Systems Engineering Processes* used for developing systems, products, components, and services and for protecting organizations, systems, and individuals.

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

Initial Comment Analysis

Themes

- New structure of XX-1 controls
- Mixed feedback on calling out "security and privacy" in controls
- High demand for track changes version and XML version of controls
- Suggestions to add controls to various baselines
- Suggestions for new controls / control enhancements
- Feedback to include baseline allocation back into control text
- Requests for mappings to other control sets/standards
- Request for additional clarity in supplemental guidance and org-defined parameters
- Suggestions for technology or implementation-specific controls (e.g., cloud, ICS)
- Request for rationale for changes

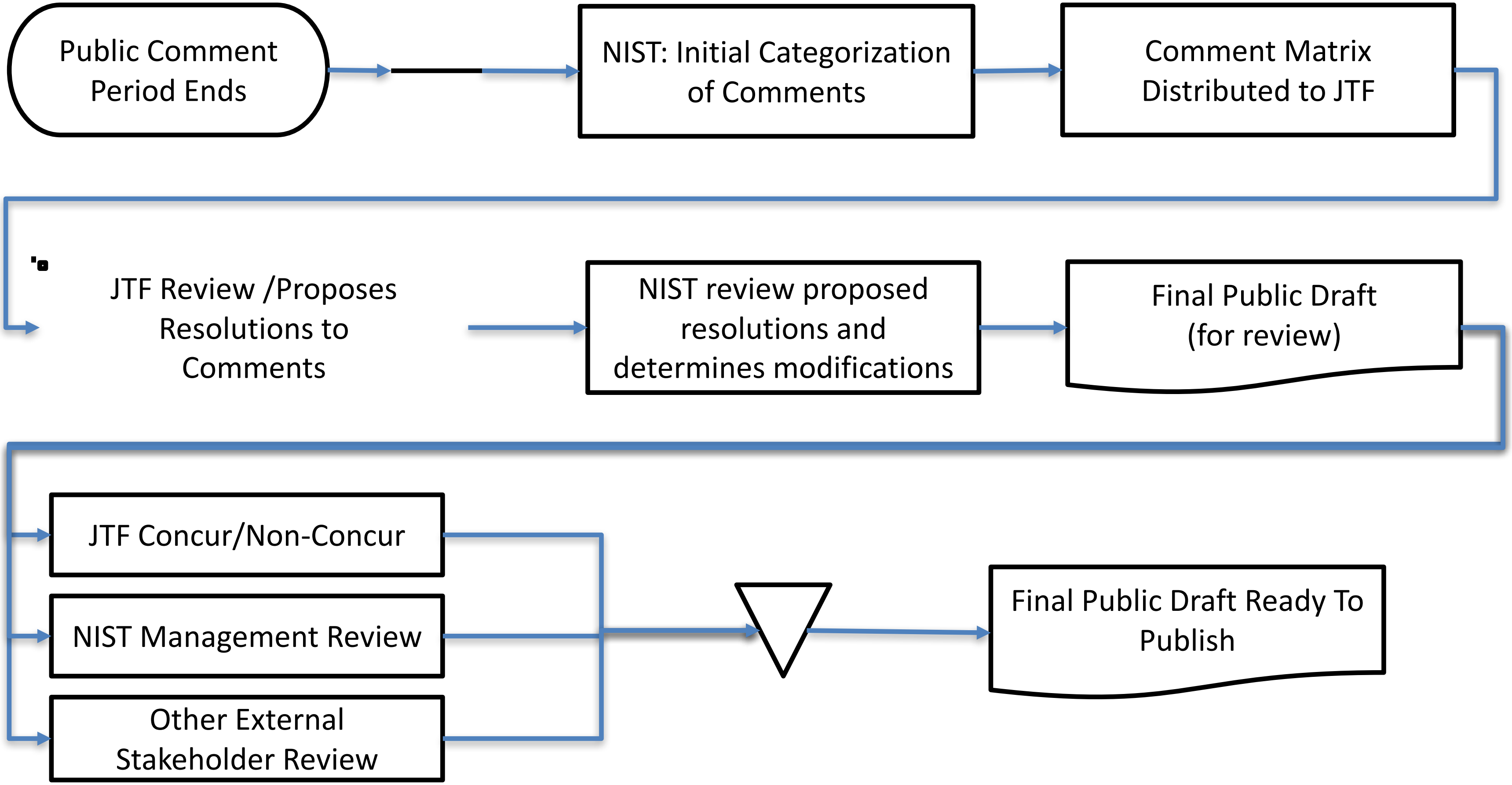
Initial Comment Analysis (Cont.)

Themes

- Some comments out of scope – issues with policy that is outside of NIST purview (that impact NIST publications and stakeholders)

  – request for implementation and assessment guidance
- Call for greater integration of privacy and security controls (e.g., removing the privacy-specific family distinctions)
- Request for more clarity regarding privacy/security overlap and differences as related to control selection and roles and responsibilities
- Support for the mapping of privacy controls to A-130 requirements

Initial Public Draft Comment Adjudication



Public Comment Period Ends

NIST: Initial Categorization of Comments

Comment Matrix Distributed to JTF

JTF Review /Proposes Resolutions to Comments

NIST review proposed resolutions and determines modifications

Final Public Draft (for review)

JTF Concur/Non-Concur

NIST Management Review

Other External Stakeholder Review

Final Public Draft Ready To Publish

Next Steps

- NIST and the JTF Partners continue to adjudicate comments

- Ongoing SME and stakeholder meetings to inform comment resolution
  - Working with OIRA, OMB, GSA in addition to the JTF partners

- *Current proposal to publish a Final Public Draft in December 2018*

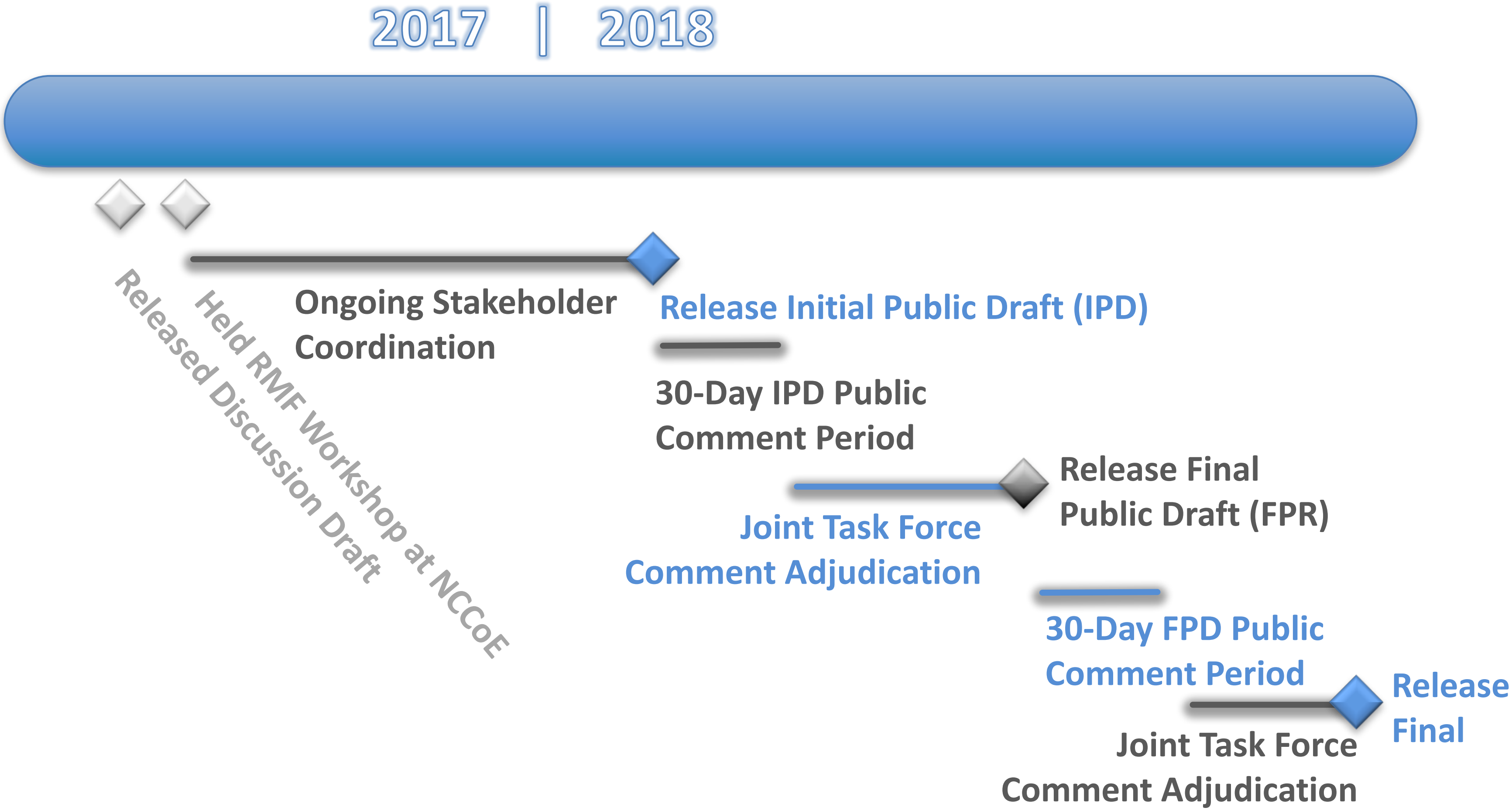
Update on Draft SP 800-37, Rev. 2

- Discussion Draft of SP 800-37, Rev. 2: *Risk Management Framework (RMF) for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, released Sept. 28, 2017
  - In response to EO 13800 and OMB M-17-25
- Leveraged the RMF Interagency Working group to provide initial feedback based on agency implementation experience
- Hosted open workshop at the NCCoE on Oct. 3, 2017 to get stakeholder input on the RMF
- Proposed (Major) Changes
  - Integration of privacy into document
  - New "Organizational Preparation" Step
  - New type of "Authorization Decisions"
    - Authorization to Use
  - Integration of Ongoing Authorization Guidance into document

Update on Draft SP 800-37, Rev. 2 (Cont.)

- Major Objectives of Update:
  - Closer linkage to risk management processes and activities at C-suite level and system/operational level (including SP 800-39)
  - Institutionalize enterprise-wide risk management prep activities
  - Demonstrate how the Cybersecurity Framework can be implemented using established NIST risk management processes
  - Integration of privacy risk management concepts into the RMF and support use of consolidated security and privacy controls in draft SP 800-53, Rev. 5

Planned SP 800-37, Rev. 2 Publication Schedule*



2017 | 2018

Released Discussion Draft

Held RMF Workshop at NCCoE

Ongoing Stakeholder Coordination

Release Initial Public Draft (IPD)

30-Day IPD Public Comment Period

Joint Task Force Comment Adjudication

Release Final Public Draft (FPR)

30-Day FPD Public Comment Period

Joint Task Force Comment Adjudication

Release Final

**Awaiting OMB Approval; Dates subject to change*

Questions and Open Discussion