



# Connecting the Dots NIST Guidance to Zero Trust

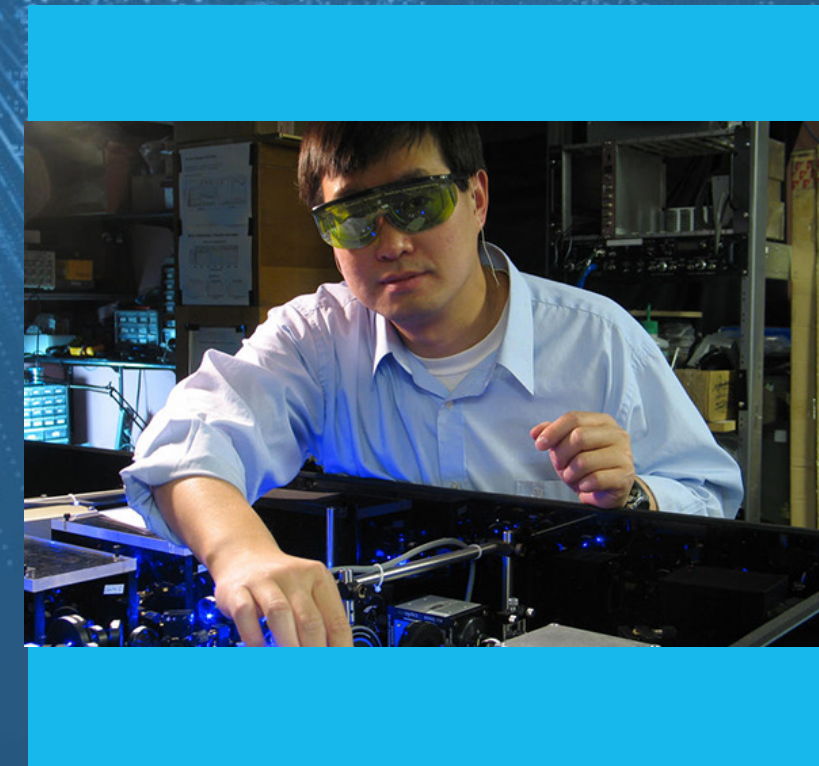
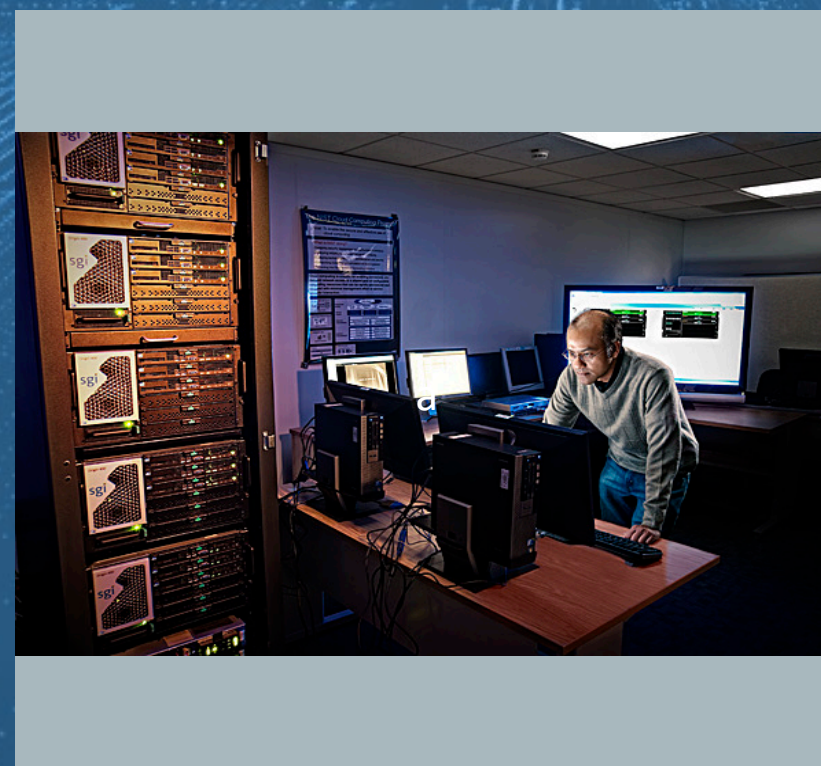
September 6, 2023

Victoria Yan Pillitteri  
[victoria.yan@nist.gov](mailto:victoria.yan@nist.gov)



# NIST MISSION

To promote U.S. innovation and industrial competitiveness by advancing  
**measurement science, standards, and technology**  
in ways that enhance economic security and improve our quality of life





# ZERO TRUST

A collection of concepts and ideas designed to minimize uncertainty in ***enforcing accurate, least privilege per-request access decisions*** in systems and services in the face of a network viewed as compromised.



# CYBERSECURITY RESOURCES THROUGH THE YEARS

NIST resources support the Zero Trust paradigm long before “Zero Trust”

1970s



1977

First authentication guideline

NBS publishes DES, first standardized encryption standard

1980s



1985

NBS issues FIPS 112, Password Usage Standard

1990s



1992

NIST introduces Role-based Access Control (RBAC)

2000s



2004

NIST releases the Risk Management Framework (RMF)

2010s



2014

NIST publishes the Cybersecurity Framework 1.0

2020s

NIST issues Zero Trust Architecture



# ZERO TRUST CHALLENGES

- ✓ Leveraging existing investments and balancing priorities
- ✓ Impact to operations or user experience
- ✓ Perception about applicability
- ✓ ZTA is not one size fits all
- ✓ Lack of standardized policy to distribute, manage, and enforce security policy
- ✓ Understanding the attack surface
- ✓ Interoperability issues
- ✓ Lack of adequate asset inventory, granular role management
- ✓ Complexity of IT communication flows and distributed components
- ✓ Visibility into communication and usage patterns
- ✓ Integrating different commercially available technologies and identifying technology gaps



# RISK MANAGEMENT AND ZERO TRUST



- ✓ risk assessment
- ✓ inventory of resources
- ✓ authorization boundary
- ✓ Requirements definition and allocation
- ✓ enterprise architecture

- ✓ controls met by policy enforcement point (PEP)

- ✓ **NIST publications provide additional implementation guidance for controls**

- ✓ Monitor current activity and state of resources

- ✓ ZT requires continuous assessment of controls (and processes)



# NEW RESOURCES AND UPCOMING EVENTS



## PUBLICATIONS

<https://csrc.nist.gov/publications>

- Draft SP 1800-35D, Implementing a Zero Trust Architecture: Functional Demonstration Plan
- Draft Interagency Report 8477, Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines



## ONLINE RESOURCES

### Online Informative References Program

<https://csrc.nist.gov/Projects/olir>

- Online reference for NIST and user-submitted mappings

### Submit Comments on SP 800-53 Controls

<https://nist.gov/rmf>

- Meet the future of public comments



## EVENTS

### Journey to the NIST Cybersecurity Framework 2.0 | Workshop #3

September 19-20, 2023

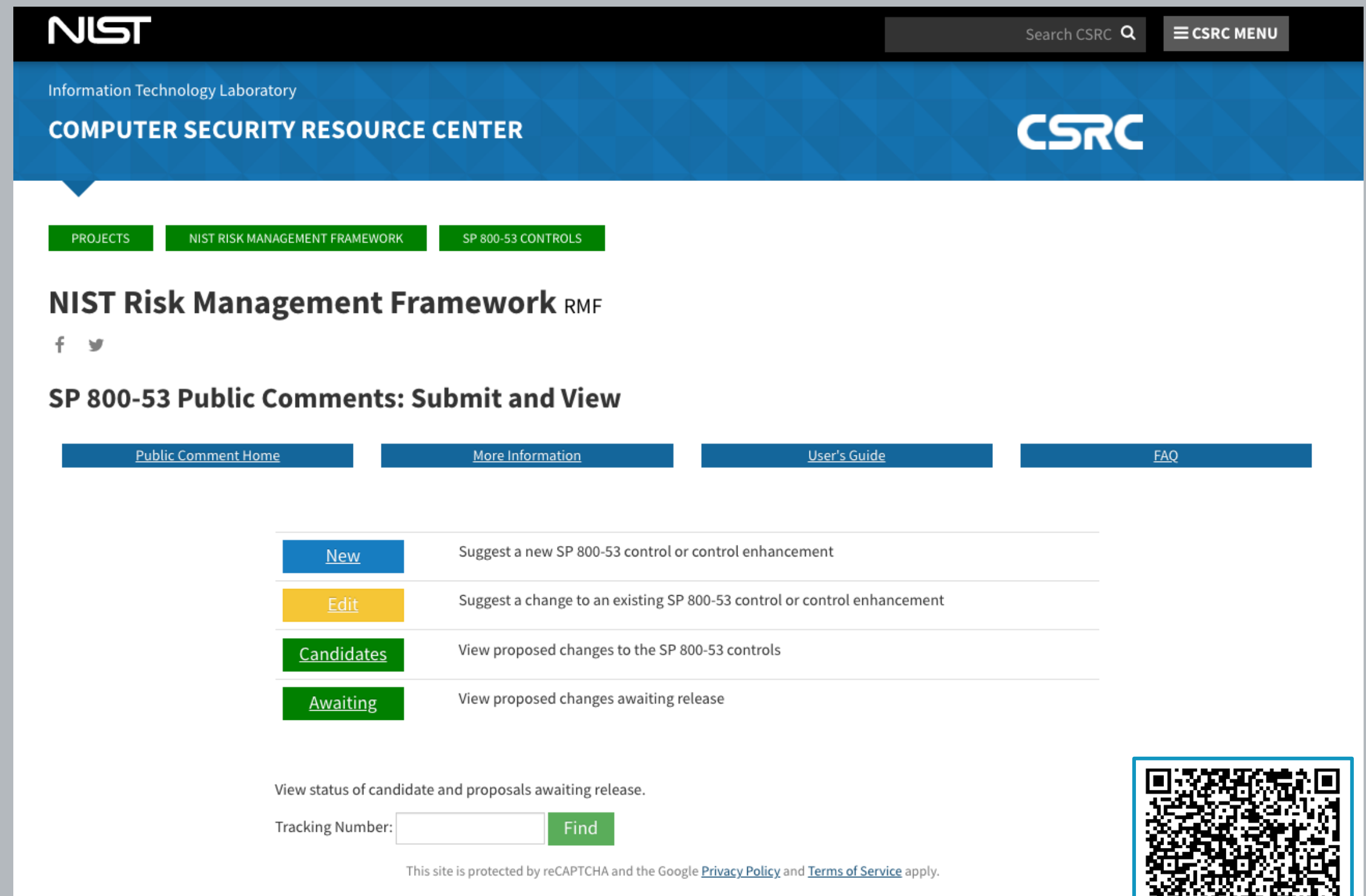
Day 1: Join by virtual livestream

Day 2: *Event at capacity (in-person only)*

# THE FUTURE OF NIST SP 800-53

## Meet the future of public comments

- > 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 submitted comments
- > Preview planned changes in next revision



The screenshot displays the NIST CSRC website. At the top, the NIST logo and 'Information Technology Laboratory' are on the left, while a search bar and 'CSRC MENU' are on the right. Below this is a blue banner with 'COMPUTER SECURITY RESOURCE CENTER' and the 'CSRC' logo. A navigation bar contains three green buttons: 'PROJECTS', 'NIST RISK MANAGEMENT FRAMEWORK', and 'SP 800-53 CONTROLS'. The main heading is 'NIST Risk Management Framework RMF' with social media icons for Facebook and Twitter. Below this is the section 'SP 800-53 Public Comments: Submit and View'. A horizontal menu has four blue buttons: 'Public Comment Home', 'More Information', 'User's Guide', and 'FAQ'. A table lists four actions: 'New' (blue button) for suggesting new controls, 'Edit' (yellow button) for suggesting changes to existing controls, 'Candidates' (green button) for viewing proposed changes, and 'Awaiting' (green button) for viewing changes awaiting release. Below the table, there is a text input field for a 'Tracking Number' and a green 'Find' button. At the bottom, a small text line 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:  [Find](#)

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

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







<https://csrc.nist.gov>

THANK YOU!