Overview of NIST Cybersecurity Standards & Guidance for Federal Agencies

Victoria Yan Pillitteri
victoria.yan@nist.gov
Computer Security Division
Overview of NIST Cybersecurity Standards and Guidance for Federal Agencies

• About the National Institute of Standards and Technology (NIST)

• NIST Cybersecurity Standards and Guidance for Federal Agencies

• Contact Information and Questions
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.
Federal Information Security Modernization Act (FISMA) Implementation Project

Established: 2003

Intended Audience: Federal agencies*

Purpose: Produce key security and risk management standards and guidelines required by Congressional legislation (FISMA 2014).

- Standards for:
  - Categorizing information and systems by mission impact
  - Minimum security requirements for information and systems

- Guidance for:
  - Selecting appropriate security controls for systems
  - Assessing security controls in systems and determining security control effectiveness
  - Security authorization of systems
  - Monitoring the security controls and the security authorizations of systems

*FISMA is applicable to federal organizations, systems and information
Information Security Risk Management Publications

Federal Information Processing Standards (FIPS)

- **FIPS 199** – Standards for Security Categorization
- **FIPS 200** – Minimum Security Requirements

Special Publications (SPs)

- **SP 800-18** – Guide for System Security Plan Development
- **SP 800-30** – Guide for Conducting Risk Assessments
- **SP 800-34** – Guide for Contingency Plan Development
- **SP 800-37** – Guide for Applying the RMF
- **SP 800-39** – Managing Information Security Risk
- **SP 800-53/53A/B** – Controls Catalog, Assessment Procedures, & Control Baselines
- **SP 800-60** – Mapping Information Types to Security Categories

- **SP 800-128** – Security-focused Configuration Management
- **SP 800-137** – Information Security Continuous Monitoring
- **SP 800-160** – Systems Security Engineering
- **SP 800-161** – Supply Chain Risk Management Practices
- **SP 800-171/A/B** – Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Assessment Procedures, & Enhanced Security Requirements

Interagency Reports (IRs)

- **NISTIR 8011** – Automation Support for Security Control Assessments
- **NISTIR 8062** – An Introduction to Privacy Engineering and Risk Management in Federal Systems
NIST Special Publication 800-39

Managing Information Security Risk – Organization, Mission, and Information System View

- Multi-tiered risk management approach
- Implemented by the Risk Executive Function
- Enterprise Architecture and SDLC Focus
- Supports all steps in the RMF
NIST Special Publication 800-30
*Guide for Conducting Risk Assessments*

- Addresses the Assessing Risk component of Risk Management (from SP 800-39)
- Provides guidance on applying risk assessment concepts to:
  - All three tiers in the risk management hierarchy
  - Each step in the Risk Management Framework
- Supports all steps of the Risk Management Framework
- A 3-step Process:
  - Step 1: Prepare for assessment
  - Step 2: Conduct the assessment
  - Step 3: Maintain the assessment
NIST Special Publication 800-37, Rev. 2


- A holistic and comprehensive risk management process
  - Can be used to communicate across an organization (C-Suite to the systems/operations)
  - Aligns the Cybersecurity Framework to the RMF
  - Includes privacy, supply chain, and security engineering

- Integrates the Risk Management Framework (RMF) into the system development lifecycle

- Provides processes (tasks) for each of the steps (Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor)
NIST Special Publication 800-53, Rev. 4
Security and Privacy Controls for Information Systems and Organizations

• Catalog of security and privacy controls
  - Not focused on any specific technologies or implementations
  - Can be applied to any kind of system

• Defines three security baselines (Low, Moderate, High)
  - Baseline for use determined by:
    ◦ information and system categorization (impact)
    ◦ organizational risk assessment and risk tolerance
    ◦ system-level risk assessment

• Some controls from the catalog are not included in any baseline

NIST SP 800-53, Rev. 5 Final Draft is currently in review – there are changes for improved usability, address emerging threats, emphasize privacy and supply chain risk management, and systems security engineering.
# NIST Special Publication 800-53, Rev. 4

*Security and Privacy Controls for Information Systems and Organizations*

## SP 800-53, Rev. 4 Control Families

<table>
<thead>
<tr>
<th>AC – Access Control</th>
<th>PL – Planning</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT – Awareness and Training</td>
<td>PM – Program Management</td>
</tr>
<tr>
<td>AU – Audit and Accountability</td>
<td>PS – Personnel Security</td>
</tr>
<tr>
<td>CA – Security Assessment and Authorization</td>
<td>RA – Risk Assessment</td>
</tr>
<tr>
<td>CM – Configuration Management</td>
<td>SA – System and Service Acquisition</td>
</tr>
<tr>
<td>CP – Contingency Planning</td>
<td>SC – System and Communication Protection</td>
</tr>
<tr>
<td>IA – Identification and Authentication</td>
<td>SI – System and Information Integrity</td>
</tr>
<tr>
<td>IR – Incident Response</td>
<td>AP* – Authority and Purpose</td>
</tr>
<tr>
<td>MA – Maintenance</td>
<td>AR* – Accountability, Audit, and Risk Management</td>
</tr>
<tr>
<td>MP – Media Protection</td>
<td>DI* – Data Quality and Integrity</td>
</tr>
<tr>
<td>PE – Physical and Environmental Protection</td>
<td>DM* – Data Minimization and Retention</td>
</tr>
</tbody>
</table>
NIST Cybersecurity Framework (CSF)

The CSF is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk.

https://www.nist.gov/cyberframework
cyberframework@nist.gov
STAY IN TOUCH

PUBLICATIONS  https://csrc.nist.gov

PROJECT INFO  https://csrc.nist.gov/Projects/Risk-Management

CONTACT  sec-cert@nist.gov  @NISTcyber