Path Forward to Support Adaption and Adoption of Cybersecurity Framework

The Framework for Improving Critical Infrastructure Cybersecurity

February 2018

cyberframework@nist.gov

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

Cybersecurity Framework *Current* Charter

Improving Critical Infrastructure Cybersecurity

Amends the National Institute of Standards and Technology Act to say:

"…on an ongoing basis, facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure"

Cybersecurity Enhancement Act of 2014 (P.L. 113-274)

18 December 2014

Key Framework Attributes

Principles of the Current and Future Versions of Framework

Common and accessible language

- Understandable by many professionals

It's adaptable to many sectors and uses

- Meant to be *customized*

It's risk-based

- A Catalog of cybersecurity outcomes
- Does provide *how or how much* cybersecurity is appropriate

It's meant to be paired

- Take advantage of great pre-existing things

It's a living document

- Enable best practices to become *standard practices for everyone*
- Can be updated as *technology and threats* change
- Evolves *faster* than regulation and legislation
- Can be updated as stakeholders *learn from implementation*

Signs of Use

Framework for Improving Critical Infrastructure Cybersecurity

- Used by over 30% of U.S. organizations, trending to 50% (Gartner, 2015, https://www.gartner.com/webinar/3163821)
- Required within the United States federal government
- Japanese translation by Information-technology Promotion Agency
- Italian translation and adaptation within Italy's National Framework for Cybersecurity
- Hebrew translation and adaptation by Government of Israel
- Bermuda uses it within government and recommends it to industry
- Focus of International Organization for Standardization & International Electrotechnical Commission

Strategic Focus Areas

Selected for Special Attention 2017-18

Small Businesses

- Drivers of the digital economy
- Prime targets for hackers
- Fewer resources and cybersecurity capabilities than larger firms

International Organizations and Governments

- Stakeholders want alignment to avoid burdensome (redundant/conflicting/costly) law and regulation
- Awareness has increased, actual alignment and use still growing

Regulatory Environments

- Regulators and regulated firms seek healthy and efficient regulatory dialogues
- Varying regulator use of Framework causes confusion

Federal Agencies

- Requirement from Executive Order 13800
- Agencies need clarity about the Framework and its relationship to NIST requirements/guidance

Small Business Guidance and Initiatives

Framework for Improving Critical Infrastructure Cybersecurity

Small Business Information Security: the Fundamentals

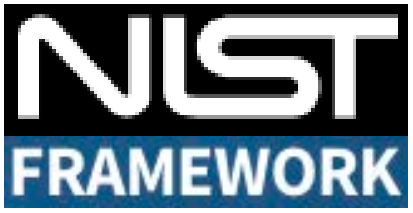
NIST Computer Security Resource Center

Small Business Center

NIST Computer Security Resource Center

CyberSecure My Business

National Cyber Security Alliance



Small Business Starter Profiles

NIST Framework Team

International Dialogs

Framework for Improving Critical Infrastructure Cybersecurity

- Japanese translation by Information-technology Promotion Agency
- Italian translation and adaptation within Italy's National Framework for Cybersecurity
- Hebrew translation and adaptation by Government of Israel
- Bermuda uses it within government and recommends it to industry
- Focus of International Organization for Standardization & International Electrotechnical Commission

Supporting Healthy Regulatory Environments

Framework for Improving Critical Infrastructure Cybersecurity

Bulk Liquid Transport Profile
U.S. Coast Guard

Financial Services Framework Customization and Profile
Financial Services Sector Coordinating Council

Connected Vehicle Profile
U.S. Department of Transportation Smart City Pilot

Baldrige Cybersecurity Excellence Builder
Baldrige Performance Excellence Program

Small Business Guidance and Initiatives

Framework for Improving Critical Infrastructure Cybersecurity

FY 2015-16 Guidance on Federal Information Security and Privacy Management Requirements

Cybersecurity Strategy and Implementation Plan

OMB Memorandum M-16-03 & 04

Managing Information as a Strategic Resource

OMB Circular A-130 Update

Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

Executive Order 13800

The Cybersecurity Framework: Implementation Guidance for Federal Agencies

Draft NIST Interagency Report 8170

Increasing Understanding and Use

Framework for Improving Critical Infrastructure Cybersecurity

- **Play to Our Strengths**
  - Governance and Enterprise Risk Management
  - Measuring Cybersecurity
  - Referencing Techniques
- **Provide Decision-to-Use Materials**
  - Success Stories
  - Quotes & Surveys
- **Making Framework Easier to Understand and Use**
  - Framework V1.1
  - Roadmap V1.1
  - Framework V1.1 in Spanish
- **Optimizing Outreach**
  - Partnerships as a Force Multiplier
  - Online Learning

Plans for the Near-Term

NIST Framework Team Fiscal Year 2018 Plan

- Winter 2018 – Finish Proposed Update Comment Analysis
- Winter 2018 – Website Update:
  - Online Informative References
  - Perspectives
  - Online Learning Materials
  - Success Story Templates
- Spring 2018 - Finalize Framework and Roadmap Version 1.1
- Spring 2018 - Finalize NIST IR 8170
- Summer 2018 – Spanish Language Framework Version 1.1
- Summer 2018 – Annual Framework Workshop
- Winter 2018-19 – Small Business Starter Profiles

Resources

Where to Learn More and Stay Current

Framework for Improving Critical Infrastructure Cybersecurity and related news and information:
www.nist.gov/cyberframework

Additional cybersecurity resources:
http://csrc.nist.gov/

Questions, comments, ideas:
cyberframework@nist.gov

If Time Permits

Input and Milestones to the Proposed Updates

Draft Framework and Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1

- December 2015 request for information – 105 comments
- April 2016 Workshop - 650+ participants
- January 2017 draft #1 of proposed updates - 129 comments
- May 2017 Workshop - 600+ participants
- December 2017 draft #2 of proposed updates - 89 comments

- Ongoing lessons learned from:
  - Framework use
  - Shared resources by NIST and industry partners
- Advances in areas identified in the 2014 Roadmap for Improving Critical Infrastructure Cybersecurity

…learned through collaborations, meetings, and events

Framework Proposed Updates

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

- Affirms Cybersecurity Enhancement Act of 2014 as the current chartering document
- Applicability to "technology" and defines technology
- Applicability for all system lifecycle phases
- Administratively updates the Informative References
- New guidance for self-assessment
- Enhanced guidance for managing cybersecurity within supply chains and for buying decisions
- Better accounts for Authorization, Authentication, and Identity Proofing
- Accounts for emerging vulnerability information (a.k.a., Coordinated Vulnerability Disclosure)
- Clarity on Implementation Tiers and their relationship to Profiles