Current State

Framework for Improving Critical Infrastructure Cybersecurity

May 2017

cyberframework@nist.gov

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

Recent Events

Key NIST Efforts Since the 2016 Workshop

Jun 2016	Published 2016 **Workshop Summary**
Sep 2016	Published draft of **Manufacturing Profile**
Nov 2016	Supported U.S. Coast Guard publication of **Maritime Bulk Liquid Transport Profile**
Jan 2017	Published **Proposed Updates** to Cybersecurity Framework
Jan 2017	Supported the University of Foscari Venice and CINI Cybersecurity National Laboratory at **ITASEC 2017**
Feb 2017	Promoted Proposed Updates at **RSA USA 2017**
Mar 2017	Hosted **Webcast** presentation on Cybersecurity Framework Overview & The Proposed Updates
Apr 2017	Published Final Version 1.0 of Baldrige **Cybersecurity Excellence Builder**
Apr 2017	Hosted Cybersecurity Excellence **Builder Workshop**
May 2017	Published Draft **Interagency Report 8170** in response to Cybersecurity Executive Order
May 2017	Published **Analysis of Request for Comment responses**

Recent NIST Work Products

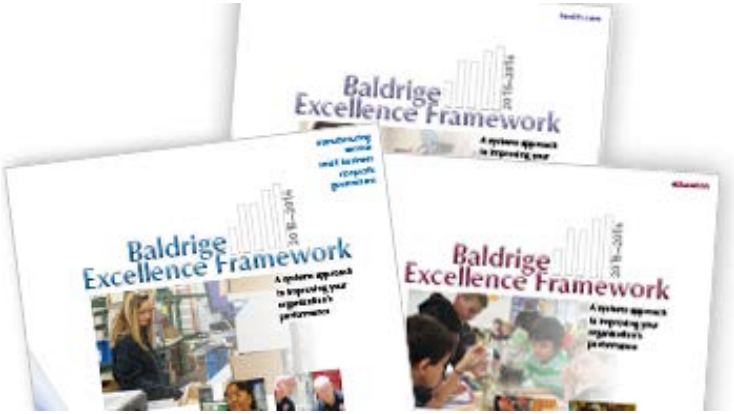
www.nist.gov/cyberframework/industry-resources

Manufacturing Profile

NIST Discrete Manufacturing Cybersecurity Framework Profile

Self-Assessment Criteria

Baldrige Cybersecurity Excellence Builder



Maritime Profile

U.S. Coast Guard Bulk Liquid Transport Profile

Future Events

Planned Future NIST Efforts After the 2017 Workshop

Jun 2017	Publish 2017 **Workshop Summary**
Jun 2017	Hosting the **Federal Computer Security Managers** Forum Annual Meeting (federal employees and designated contractors only)
Jul 2017	Support the **Bermudan Workshop** on Cybersecurity Framework
Summer 2017	Publish a **"How To" guide** on creating Cybersecurity Framework Profiles
Summer 2017	Support the Joint Task Force publishing draft Special Publication **800-37 Revision 2** integrating Cybersecurity Framework
Oct 2017	Support the **European Cybersecurity Forum**
TBA	Publish **Version 1.1** of Cybersecurity Framework
TBA	Support U.S. Coast Guard publication of additional **maritime Profiles**
2018	Publish **"Starter Profiles"** to support small businesses

The Next Version…

Framework for Improving Critical Infrastructure Cybersecurity

May 2017

cyberframework@nist.gov

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

Presiding Thoughts

Use and customize Framework in any way that provides value

NIST depends upon – and uses – your input

Framework is private sector-driven

Evolution is vital to our continued success

Input to the Proposed Framework Update

Draft Update based on feedback including:

- **December 2015 request for information**
- **April 2016 workshop**
- **Lessons learned from Framework use**
- **Shared resources from industry partners**
- **Advances in areas in the Roadmap issued with the Framework in February 2014**
- **Proposed Update published in January 2017**
- **Comments received by April 2017**

Intent Overall: Still the Same

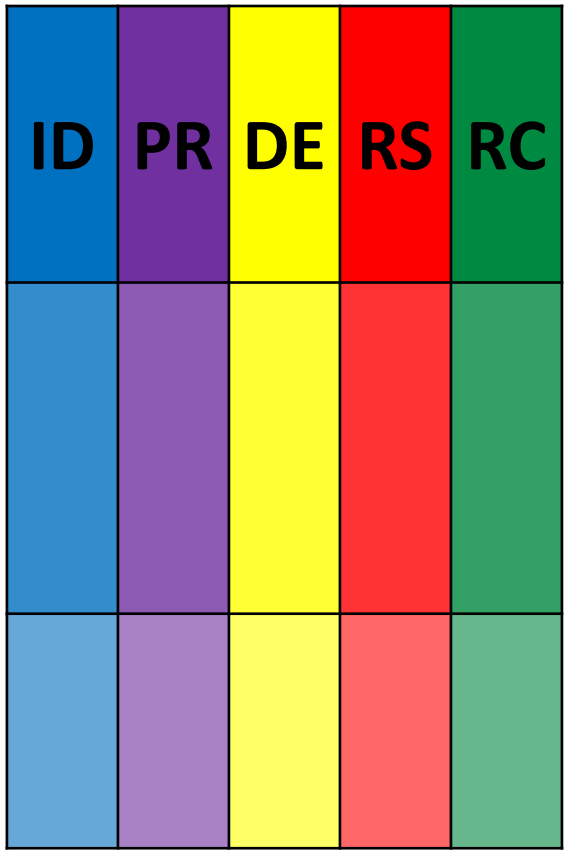
- Customizable
- Provides *common language* and systematic methodology for managing cyber risk
- Does not indicate *how* much cyber risk is tolerable, nor provide “one and only” formula for cybersecurity
- Enables best practices to become *standard practices for everyone* via common lexicon to enable action across diverse stakeholders
- Reduces need for versioning by designing the Framework to be technology and architecture agnostic
- Living document: easy to update, *learn from use,* revise as *technology and threats* change

Intent Overall: Backward Compatibility

Interoperable and compatible with version 1.0

Less Variation

More Variation

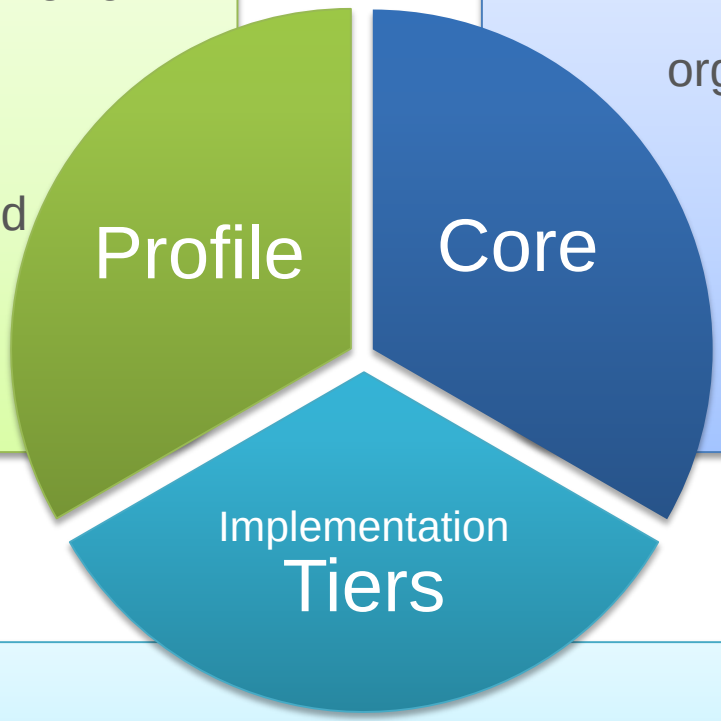


Adds – ok
Deletes – ok
Enhancements – ok
Changes/Moves –not ok

Cybersecurity Framework Components

Aligns industry standards and best practices to the Framework Core in a particular implementation scenario

Supports prioritization and measurement while factoring in business needs



Cybersecurity activities and informative references, organized around particular outcomes

Enables communication of cyber risk across an organization

Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

Placement within Framework

IF	*THEN*
High-level actions, practices, behaviors	Implementation Tiers
Outcomes	Core
Detailed, broad, widely-used guidance or standards	Informative References
Description of Framework components	Section 2
High-level description of Framework use	Section 3
Basic clarifications; relationships & compatibility with… ; niche use	Frequently Asked Questions
Independent initiatives, administered in alignment with Framework	Roadmap

Intent: Supply Chain Risk Management

Intent

- Provide many possible ways for Cyber SCRM to be included

Proposed Update Summary

- Expanded descriptive narrative
- Added process
- Added an entity taxonomy
- Added a property to Implementation Tiers
- Added a Category to the Core

Seeking Input On…

- Too much?
- How to best address non-contractual relationships (a.k.a. external dependencies)

Intent: Measurement

Intent

- Add much-requested options for measurement
- Enable use of detailed measurement that lives outside of Framework
- *For self-use:* self-assessment and/or assessment of your suppliers

Proposed Update Summary

- Added four word taxonomy

Seeking Input On…

- How to add measurement without pulling Framework toward compliance-based approach?

Intent: Identity Management

Intent

- Ensure complete coverage of Identity Management in Framework

Proposed Update Summary

- Enhanced Category and Subcategory pre-existing wording
- Added Subcategory on Identity Proofing

Seeking Input On…

- How to better integrate authentication
- Whether/How to integrate multi-factor authentication

Intent: Implementation Tiers & Profiles

Intent

- Provide enough detail to better relate the two
- Not so much to make if constraining or formulaic

Proposed Update Summary

- Additional Actions in “hourglass diagram” (Figure 2)
- Additional prose in Seven Step Process (Steps 1 & 5)

Seeking Input On…

- How to make the relationship between Implementation Tiers and Profiles clear, without being prescriptive?

Formal Comments Received

- **NIST received 129 written comments from:**
  - Individuals
  - Organizations
    - Mostly private sector
    - Some government
    - International as well as U.S.
  - Industry groups/trade associations representing many companies

Comment Analysis

Labeling of the Framework

- Re-title Framework, deleting “critical infrastructure” to convey that it is useful more broadly

Section 2.2 Implementation Tiers

- Continue to refine and clarify the value and use of Implementation Tiers
- Add guidance or use cases

Supply Chain Risk Management (SCRM)

- Addition of SCRM to the Framework generally viewed as positive and needed
- Additional examples, use cases, and references would be helpful to further clarify SCRM use in the Framework

Comment Analysis

Section 4.0 Measuring and Demonstrating Cybersecurity

- Adding measurement section deemed important by many; further development recommended
- Label measurement section to clearly indicate that measurement provisions should be for *internal or self-assessment use*
- Take care to ensure continued risk-based application of the Framework -- and to avoid compliance-based application
- Changes in “categories” of measurement recommended
- Some suggested less emphasis on quantitative measurement

Comment Analysis

Appendix A: Framework Core

- Respondents affirmed integration of SCRM into the Core. Some suggested SCRM be integrated across existing Categories, rather than adding an SCRM Category to the Identify Function
- Respondents affirmed the enhancement of the Identity Management, Authentication and Access Control Category and provided further thoughts for consideration
- Modify and improve usefulness of Informative References; define the process for determining future Informative References

Comment Analysis

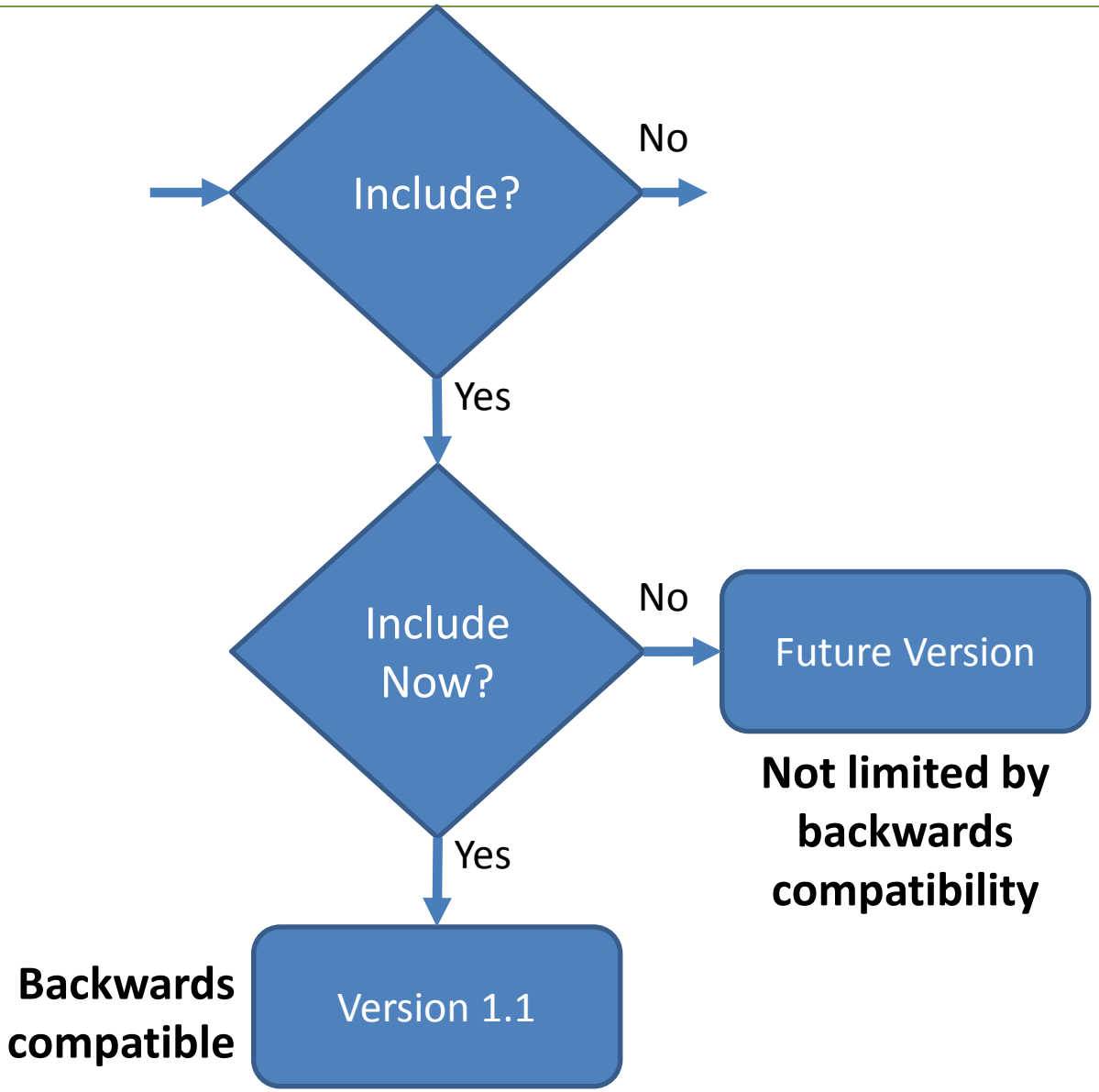
Small Business Prioritization

- NIST should continue to support Small Business involvement with the Framework and provide greater clarity about how smaller businesses can use the Framework.

Global Outreach Efforts

- NIST should continue to promote the Framework internationally in the interest of alignment and common approach.

Triaging Proposed Changes



Places to Update

- Cybersecurity Framework document
- Roadmap
- CSF Reference Tool
- Frequently Asked Questions
- Additional documents

Next steps for the Proposed Update

- Request for Comment analysis: May 2017
- Workshop: May 2017
- Analysis of further comment during workshop
- Publish a final version of 1.1
- How/when to approach version 2.0

Presiding Thoughts

Use and customize Framework in any way that provides value

NIST depends upon – and uses – your input

Framework is private sector-driven

Evolution is vital to our continued success