Beyond the Basics: Exploring NIST Cybersecurity Framework 2.0

Daniel Eliot, NIST
Stephen Quinn, NIST

January 22, 2025

NIST Cybersecurity Framework 2.0

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Guidance that helps organizations—regardless of size, sector, or maturity— better **understand, assess, prioritize**, and **communicate** their cybersecurity efforts.

CSF Core

Cybersecurity outcomes that can help any organization manage its cybersecurity risks.

Functions, Categories, Subcategories

CSF Organizational Profiles

Mechanism for describing an organization's **current and/or target cybersecurity posture** in terms of the CSF Core's outcomes.

CSF Tiers

Characterize the **rigor** of an organization's cybersecurity risk governance and management practices. Tiers can also provide **context** for how an organization views cybersecurity risks and the processes in place to manage those risks.

Nist.gov/cyberframework

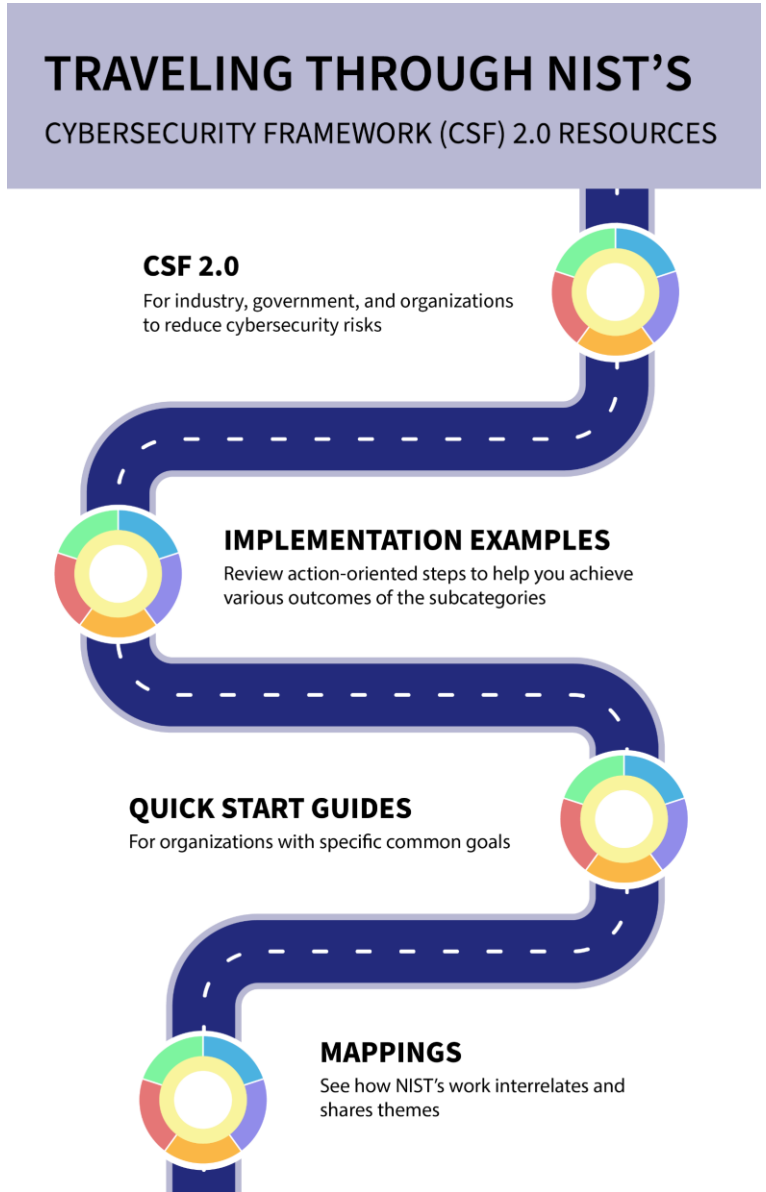
How Did We Get Here?

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

The CSF 2.0 has been developed through an iterative, community driven process since its inception in 2022.

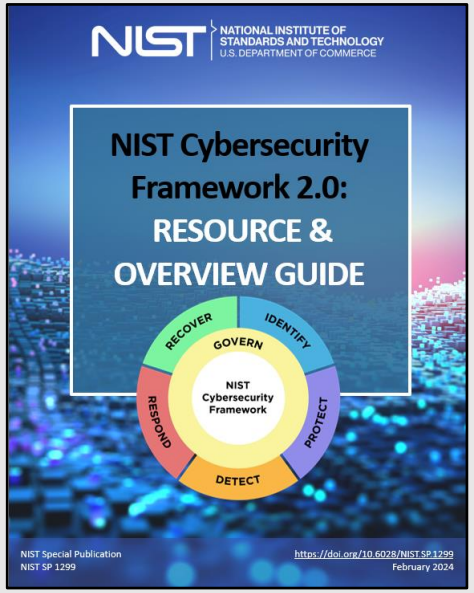
CSF 2.0 | What Makes it Different?

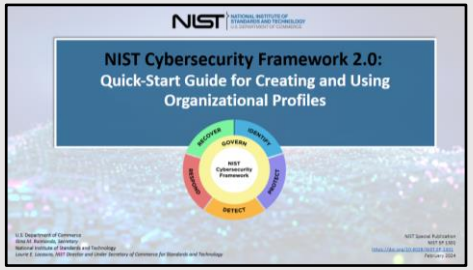
- Incorporates an entirely new function to address ***"Governing" risk management*** processes
- ***Integrates Supply Chain*** throughout the existing functions, categories, subcategories, and new resources!
- Modifies categories & subcategories to ***address specific threats and technology*** shifts.
- Shifts focus to ***how organizations can more rapidly*** implement and improve their cybersecurity posture
- Less about a single document and more about a ***suite of resources*** that aims to provide flexible, leading-edge inputs to consumers

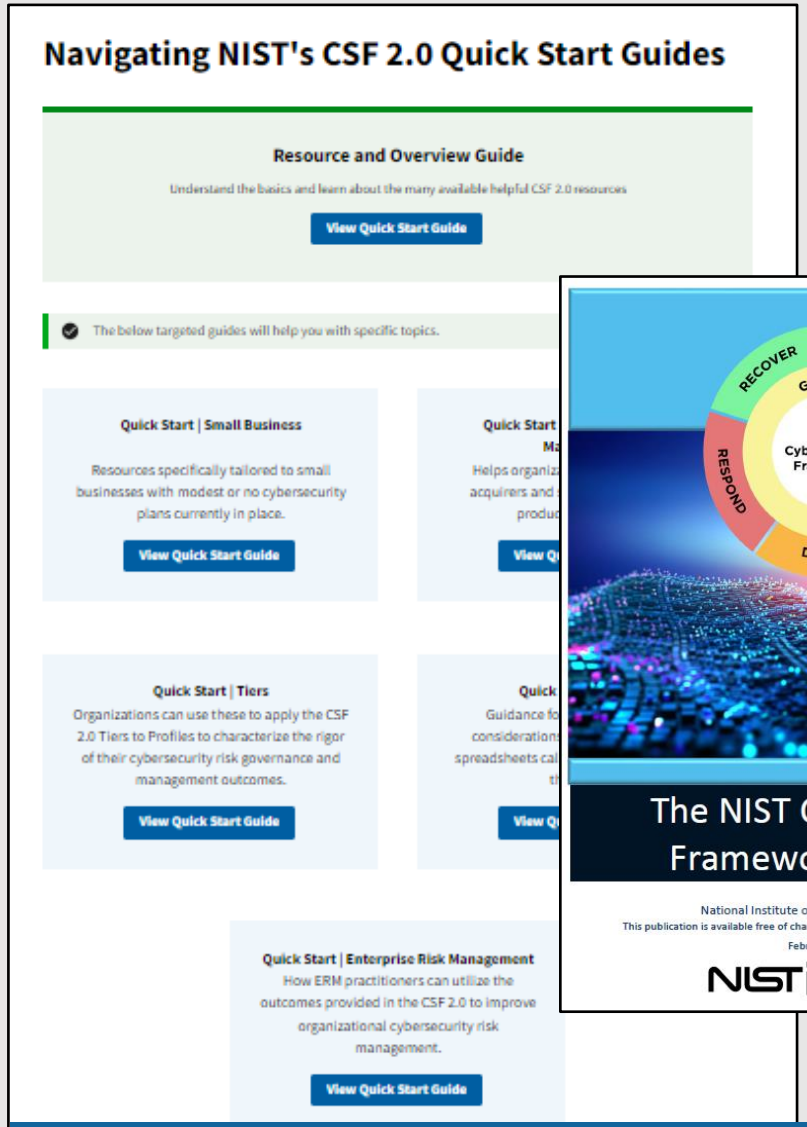


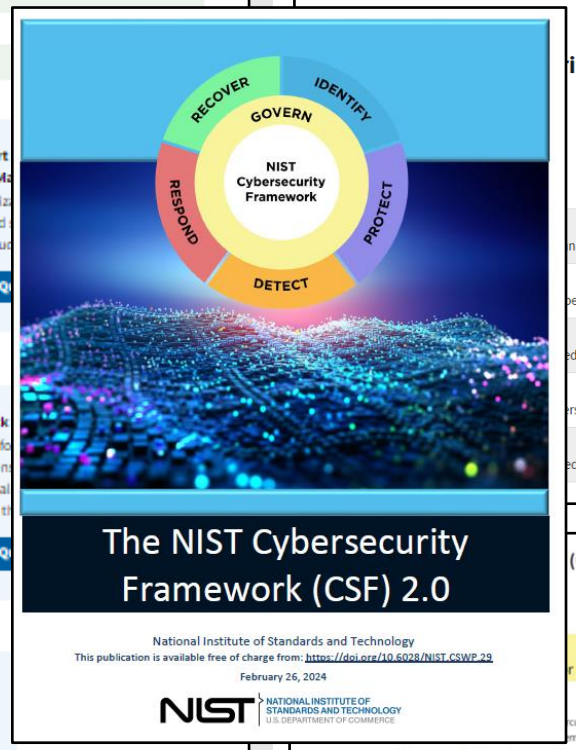
Suite of Resources Snapshot

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE









Nist.gov/cyberframework

CSF Profiles– Moving from a gap analysis of current/target state to implementation and assessment

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Understanding Your Current and Target Cybersecurity Posture

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Create Organizational Profile

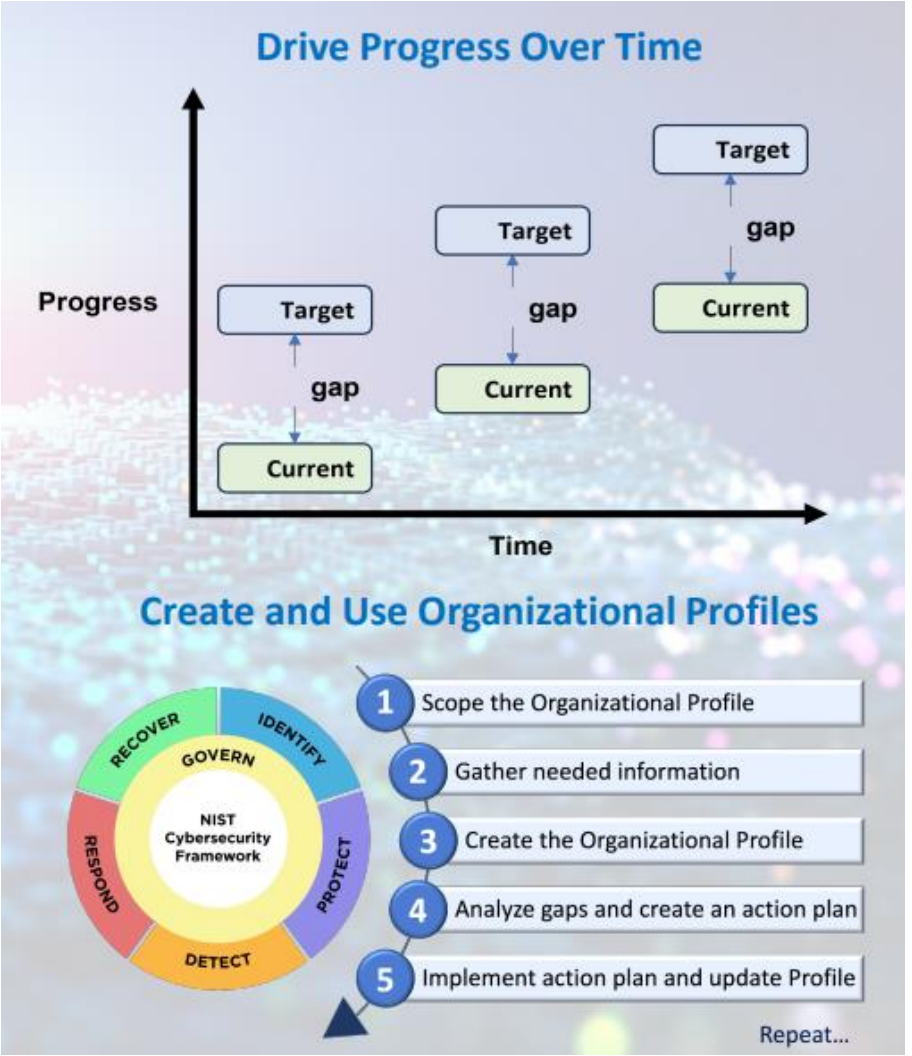
- CSF 2.0 Organizational Profiles Quick Start Guide: https://doi.org/10.6028/NIST.SP.1301

Organizational Profiles can be categorized as:

- **A Current Profile** that specifies the CSF outcomes an organization is currently achieving and characterizes how or to what extent each outcome is being achieved.

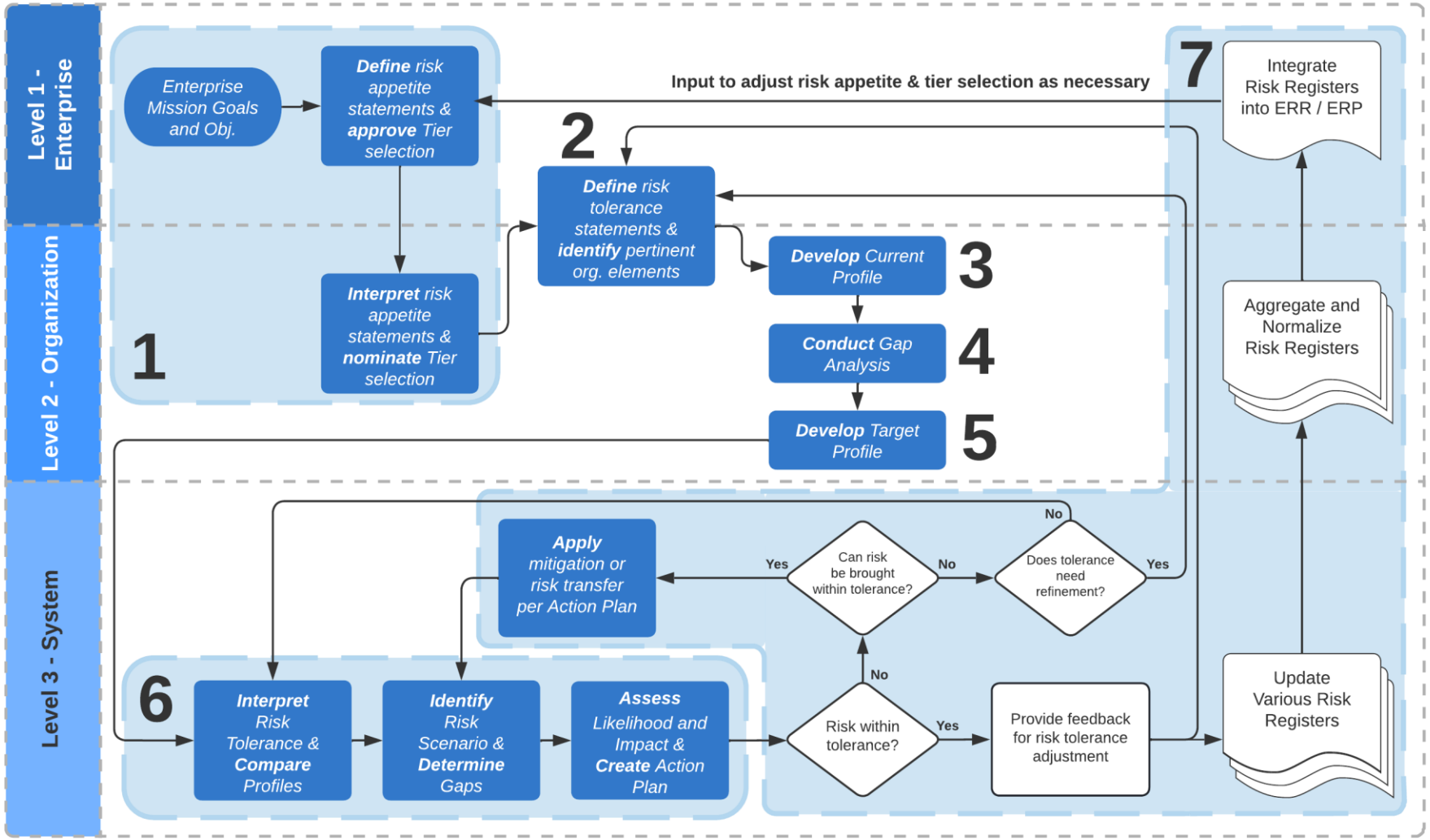
- **A Target Profile** that specifies the desired CSF outcomes an organization has selected and prioritized for achieving its cybersecurity risk management objectives.

Analyze the gaps, then create an action plan



Cybersecurity Framework steps in Support of CSRM Integration

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE



https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8286C-upd1.pdf (Figure 7)

NIST CSF 2.0: CREATING AND USING ORGANIZATIONAL PROFILES

A QUICK START GUIDE

CREATE THE ORGANIZATIONAL PROFILE – PART 2

The table below shows a notional example of a single row from an Organizational Profile. This is meant for illustrative purposes only. Here are some tips drawn from the example:

- Add and remove columns from the Organizational Profile template to suite your needs. The CSF encourages users to record whatever information is significant and to use whatever format they prefer.
- The columns do not have to be the same for the Current Profile and the Target Profile.
- Include Informative References to understand differences between Practices and Goals. This example shows SP 800-53 controls in the square brackets.

CSF Outcomes		Current Profile			Target Profile	
Identifier	**Description**	**Practices**	**Status**	**Rating**	**Priority**	**Goals**
PR.PS-01	Configuration management practices are established and applied	Policy: Configuration Management policy version 1.4, last updated 10/14/22. Defines the configuration change control policy [**CM-1**]. Procedures: System owners and technology managers informally implement configuration management practices. Change control processes are not consistently followed. The CIO specifies configuration baselines [**CM-2**] for the IT platforms and applications most widely used within the organization, but baseline use is not monitored or enforced consistently across the organization.	Configuration management is partially implemented within the organization. Some systems do not follow available baselines and other systems do not have baselines, so they may have weak configurations that make them more susceptible to misuse and compromise. Unauthorized changes may go undetected. Some changes are not tested or tracked.	3 *out of 5*	High	Policy: The Configuration Management policy requires configuration baselines to be specified, used, enforced, and maintained for all commodity technologies used by the organization. The policy requires change control processes to be followed for all technologies within the organization [**CM-1**]. Procedures: Each division of the organization has a configuration management plan [**CM-9**], as well as maintains, implements, and enforces configuration baselines [**CM-2**] and settings [**CM-6**] for their systems. Baselines are applied to all systems before production release. All systems are continuously monitored for unexpected configuration changes, and tickets are automatically generated when deviations from baselines occur. Designated parties review change requests and corresponding impact analyses [**CM-4**] and approve or deny each [**CM-3**].

Implementation and Assessment

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

A recommended approach for developing action plans is to use the NIST CSF 2.0 Reference Tool to follow the references from your Target Profile's pertinent Subcategories to the associated informative references, such as SP 800-53.

CSF 2.0 Informative References

Relationships between the Core and various best practices, including standards, guidelines, regulations, and other resources.

https://www.nist.gov/informative-references

Additional NIST Resources

- NIST IR 8286B, Prioritizing Cybersecurity Risk for Enterprise Risk Management
- NIST SP 800-37 Revision 2, Risk Management Framework for Information Systems & Organizations
- NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems & Organizations
- NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments

Implementation Examples

Subcategory	Implementation Example
GV.SC-04: Suppliers are known and prioritized by criticality	Ex1: Develop criteria for supplier criticality based on, for example, the sensitivity of data processed or possessed by suppliers, the degree of access to the organization's systems, and the importance of the products or services to the organization's mission
	Ex2: Keep a record of all suppliers, and prioritize suppliers based on the criticality criteria

https://www.nist.gov/document/csf-20-implementation-examples-xlsx

Global Impact of CSF 2.0

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Global Impact of CSF 2.0

- The CSF is used widely internationally.
- CSF 2.0 has been translated into 6 languages so far (French, German, Korean, Polish, Portuguese, and Spanish)
- The resources allow organizations to build cybersecurity frameworks and organize controls using the CSF Functions.

nist.gov/ cyberframework/translations

Frequently Asked Questions

CSF Frequently Asked Questions

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Is there a summary of major changes to the Core from version 1.1 to 2.0?
Why are there gaps in the CSF Subcategory enumeration?
Does NIST provide certification for CSF implementation or products?
Is the CSF aligned with international cybersecurity initiatives and standards? (nist.gov/informative-references) https://www.nist.gov/cyberframework/faqs

Submit your questions to: cyberframework@nist.gov

nist.gov/cyberframework/faqs

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Questions?

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

nist.gov/cyberframework

cyberframework@nist.gov