Journey to the NIST CSF 2.0

Cheri Pascoe, Director, NIST NCCoE

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

nccoe.nist.gov

Cybersecurity Framework Attributes

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The NIST Cybersecurity Framework (CSF) helps organizations reduce their cybersecurity risks and is widely recognized as foundational to securing organizations & technology.

- Cybersecurity outcomes – the “what”, not “how” or “who”
- Review priorities and gaps; align legal/regulatory requirements and organizational and risk management priorities
- Common and accessible language for communication on cybersecurity posture
- Based on and mapped to international standards and resources
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Guided by many perspectives – private sector, academia, public sector

Governmental Policies on CSF

Adapted in several countries and regions

- United States (federal and state)
  - **Executive Order 13800** – requires federal agency use of the NIST CSF
  - **The White House National Cybersecurity Strategy (March 2023): https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf**
    - "Regulations should be performance-based, leverage existing cybersecurity frameworks, voluntary consensus standards, and guidance – including the Cybersecurity and Infrastructure Security Agency (CISA)'s Cybersecurity Performance Goals and the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity – …"
- Canada
- Italy
- Poland
- Israel
- Japan
- Uruguay
- Australia and more

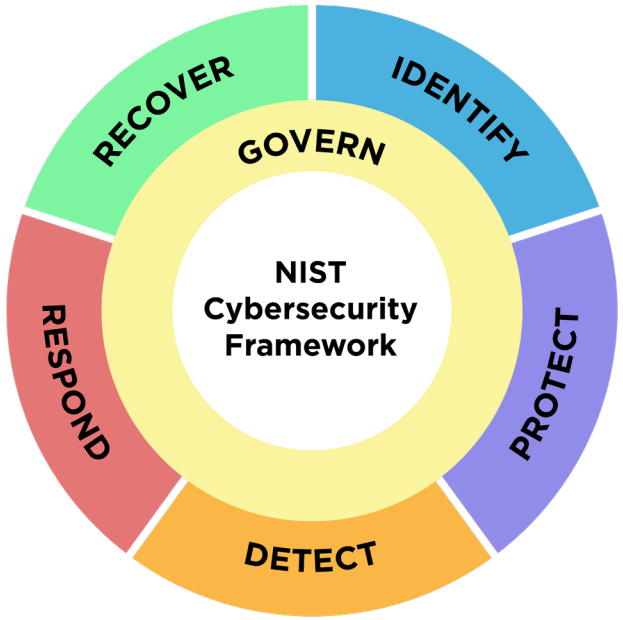
Examples highlighted on the NIST International Cybersecurity and Privacy Resource Site: https://www.nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources

CSF Update | Journey to CSF 2.0

- **NIST is updating the Cybersecurity Framework** to address the evolving cybersecurity risk and standards landscape and make it easier for organizations to address risks. NIST is actively relying on and seeking diverse stakeholder feedback in the update process.

Ways to engage: www.nist.gov/cyberframework

Draft CSF 2.0



This newly released draft represents a major update to the CSF, which was first released in 2014.

Key Updates:

- Reflects changes in the cybersecurity landscape (risks, technologies, standard changes)
- Makes it easier to put the CSF into practice for all organizations through additional guidance on implementing the CSF
- An expanded scope beyond critical infrastructure.
- The addition of a sixth function, Govern.
- Additional coverage of supply chain security.

Comments on the Draft Core may be sent to cyberframework@nist.gov by November 4, 2023.

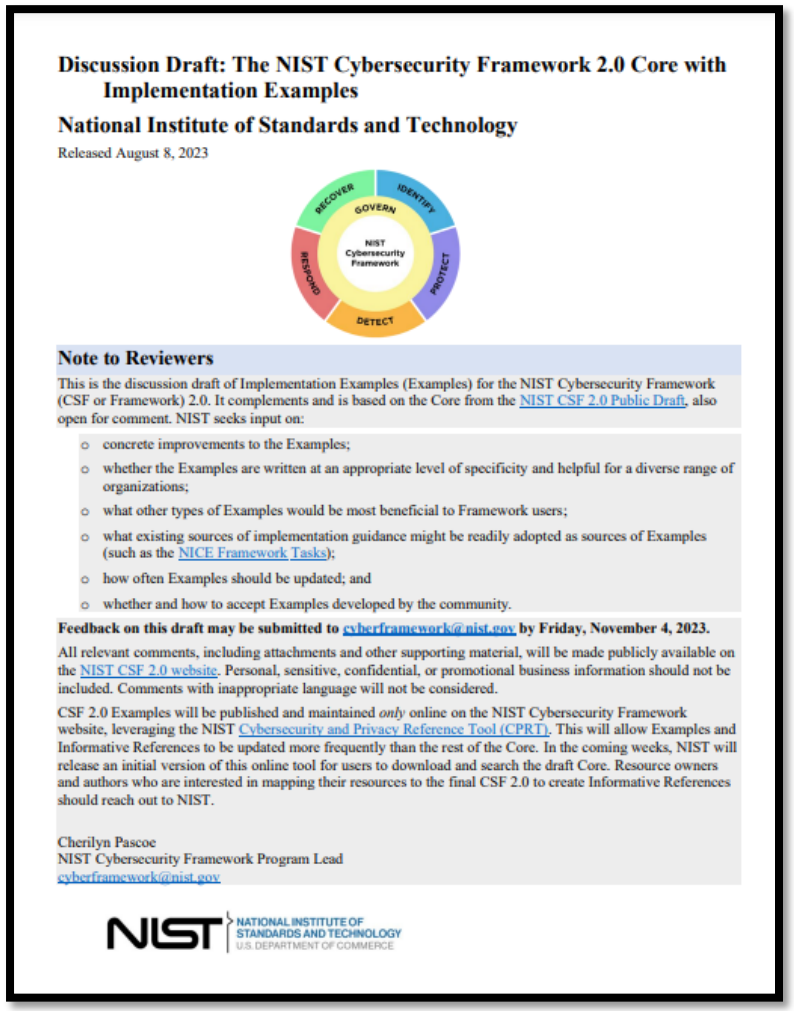
CSF 2.0 Draft Core

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Comments on the Discussion Draft may be sent to cyberframework@nist.gov by November 4, 2023.

CSF 2.0 Discussion Draft
Revised Core with Implementation Examples

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE



Discussion Draft: The NIST Cybersecurity Framework 2.0 Core with Implementation Examples

National Institute of Standards and Technology

Released August 8, 2023

Note to Reviewers

This is the discussion draft of Implementation Examples (Examples) for the NIST Cybersecurity Framework (CSF or Framework) 2.0. It complements and is based on the Core from the NIST CSF 2.0 Public Draft, also open for comment. NIST seeks input on:

- concrete improvements to the Examples;
- whether the Examples are written at an appropriate level of specificity and helpful for a diverse range of organizations;
- what other types of Examples would be most beneficial to Framework users;
- what existing sources of implementation guidance might be readily adopted as sources of Examples (such as the NICE Framework Tasks);
- how often Examples should be updated; and
- whether and how to accept Examples developed by the community.

Feedback on this draft may be submitted to cyberframework@nist.gov by Friday, November 4, 2023.

All relevant comments, including attachments and other supporting material, will be made publicly available on the NIST CSF 2.0 website. Personal, sensitive, confidential, or promotional business information should not be included. Comments with inappropriate language will not be considered.

CSF 2.0 Examples will be published and maintained *only* online on the NIST Cybersecurity Framework website, leveraging the NIST Cybersecurity and Privacy Reference Tool (CPRT). This will allow Examples and Informative References to be updated more frequently than the rest of the Core. In the coming weeks, NIST will release an initial version of this online tool for users to download and search the draft Core. Resource owners and authors who are interested in mapping their resources to the final CSF 2.0 to create Informative References should reach out to NIST.

Cherilyn Pascoe
NIST Cybersecurity Framework Program Lead
cyberframework@nist.gov

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

nist.gov/document/discussion-draft-nist-cybersecurity-framework-20-core-implementation-examples

Function

IDENTIFY (ID): Help determine the current cybersecurity risk to the organization

Category

Asset Management (ID.AM): Assets (e.g., data, hardware software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy

Subcategory

ID.AM-01: Inventories of hardware managed by the organization are maintained

Implementation Examples

Ex1: Maintain inventories for all types of hardware, including IT, IoT, OT, and mobile devices

Ex2: Constantly monitor networks to detect new hardware and automatically update inventories

Subcategory

ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained

Implementation Examples

Ex1: Maintain inventories for all types of software and services, including commercial-off-the-shelf, open-source, custom applications, API services, and cloud-based applications and services

Ex2: Constantly monitor all platforms, including containers and virtual machines, for software and service inventory changes

Ex3: Maintain an inventory of the organization's systems

Comments on the Discussion Draft may be sent to cyberframework@nist.gov by November 4, 2023.

CSF 2.0 Next Steps

- **Public workshops and events**
  - Find recordings of CSF Workshop #1 (August 2022) and #2 (February 2023) and #3 (September 2023) online.
- **Comment on drafts**
  - Provide comments on the Draft CSF 2.0 and the Core Implementation Examples Discussion Draft by November 4, 2023 (all prior comments received can be found online).
- **Continuing to seek and develop CSF resources, success stories, and mappings to other frameworks and standards.**

Helping Organizations Implement CSF 2.0

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

nccoe.nist.gov

The National Cybersecurity Center of Excellence

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Collaborate with innovators to provide **real-world, standards-based** cybersecurity capabilities that address business needs.

CSF 2.0 Profiles

- The Framework's mechanism for describing an organization's current or target cybersecurity posture in terms of the Core's outcomes is called a Framework Profile.

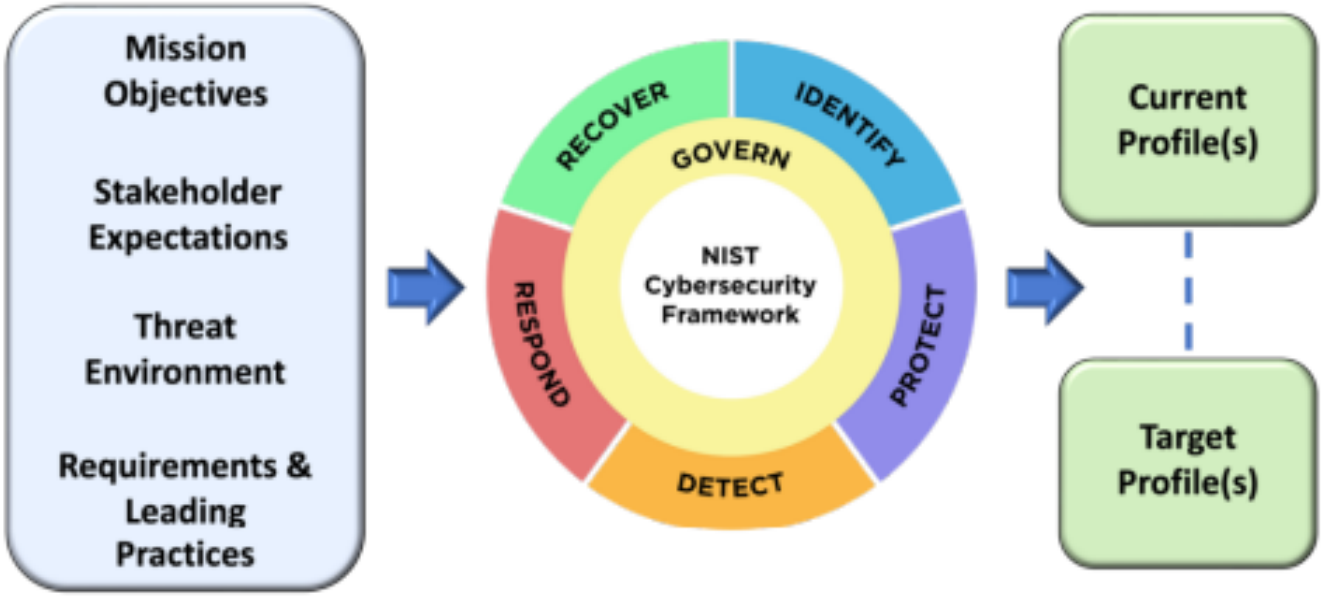


Fig. 3. Cybersecurity Framework Profiles

CSF 2.0: www.nist.gov/cyberframework

NIST Publications on CSF Profiles

A Community Profile is a Target Profile created to address shared interests and goals among a group of organizations. Organizations can consider using it as the basis for their own Target Profile. An example of a Community Profile is one developed for a sector or subsector, or for a specific use case or technology.

Recently published:

- **EV/XFC (with DOE):** Electric Vehicle (EV) Extreme Fast Charging (XFC) CSF Profile
- **Liquified Natural Gas (LNG) (with DOE):** Cybersecurity Framework Profile for Liquefied Natural Gas (NISTIR 8406)
- **Positioning, Navigation, Timing (PNT) (under EO):** Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of PNT Services (NISTIR 8323 Rev. 1)
- **Satellite Ground:** Applying the Cybersecurity Framework to Assure Satellite Command and Control (NISTIR 8401)
- **Satellite Networks (with Space Force):** Cybersecurity Profile for the Hybrid Satellite Networks (HSN) Cybersecurity (NISTIR 8441)
- **Satellite Operations**: Introduction to Cybersecurity for Commercial Satellite Operations (NISTIR 8270)
- **Ransomware Profile***:* Ransomware Risk Management: A Cybersecurity Framework Profile (NISTIR 8374)
- **Connected Vehicles (with DOT):** Cybersecurity Framework Profile for Connected Vehicles

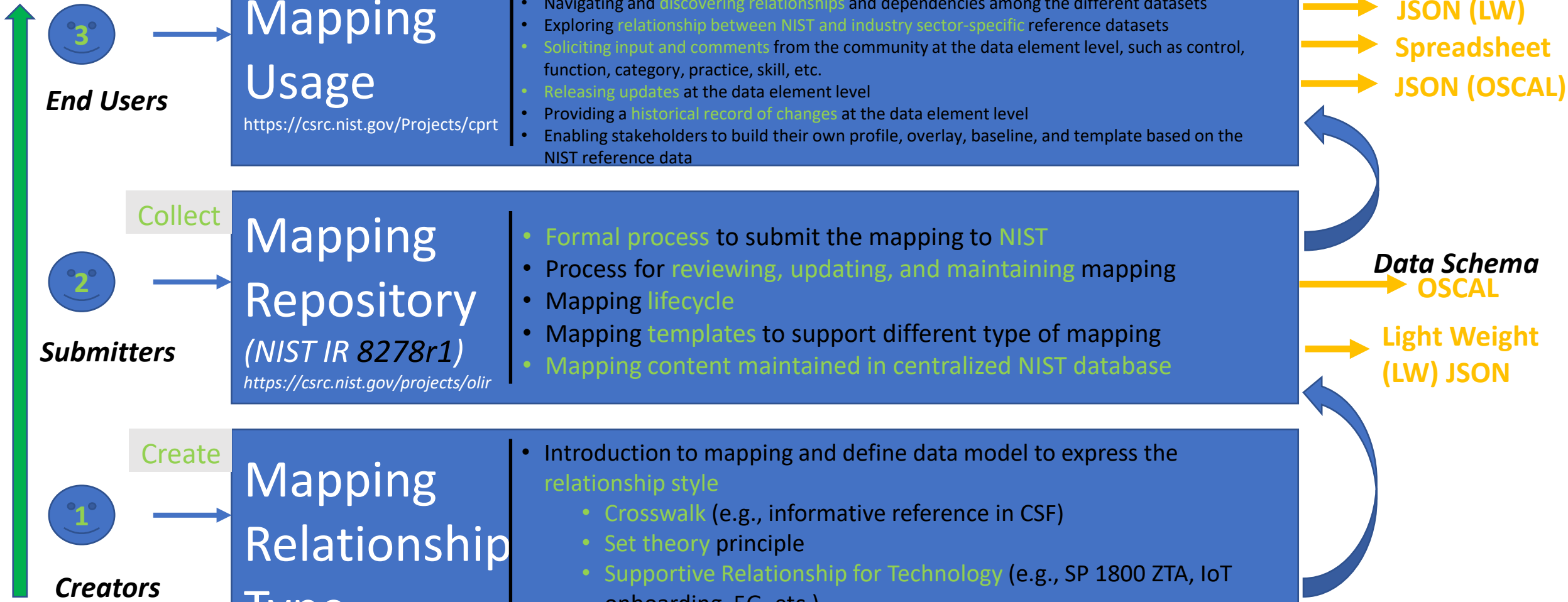
Sample of External Community Profiles

A **Community Profile** is a Target Profile created to address shared interests and goals among a group of organizations. Organizations can consider using it as the basis for their own Target Profile. An example of a Community Profile is one developed for a sector or subsector, or for a specific use case or technology.

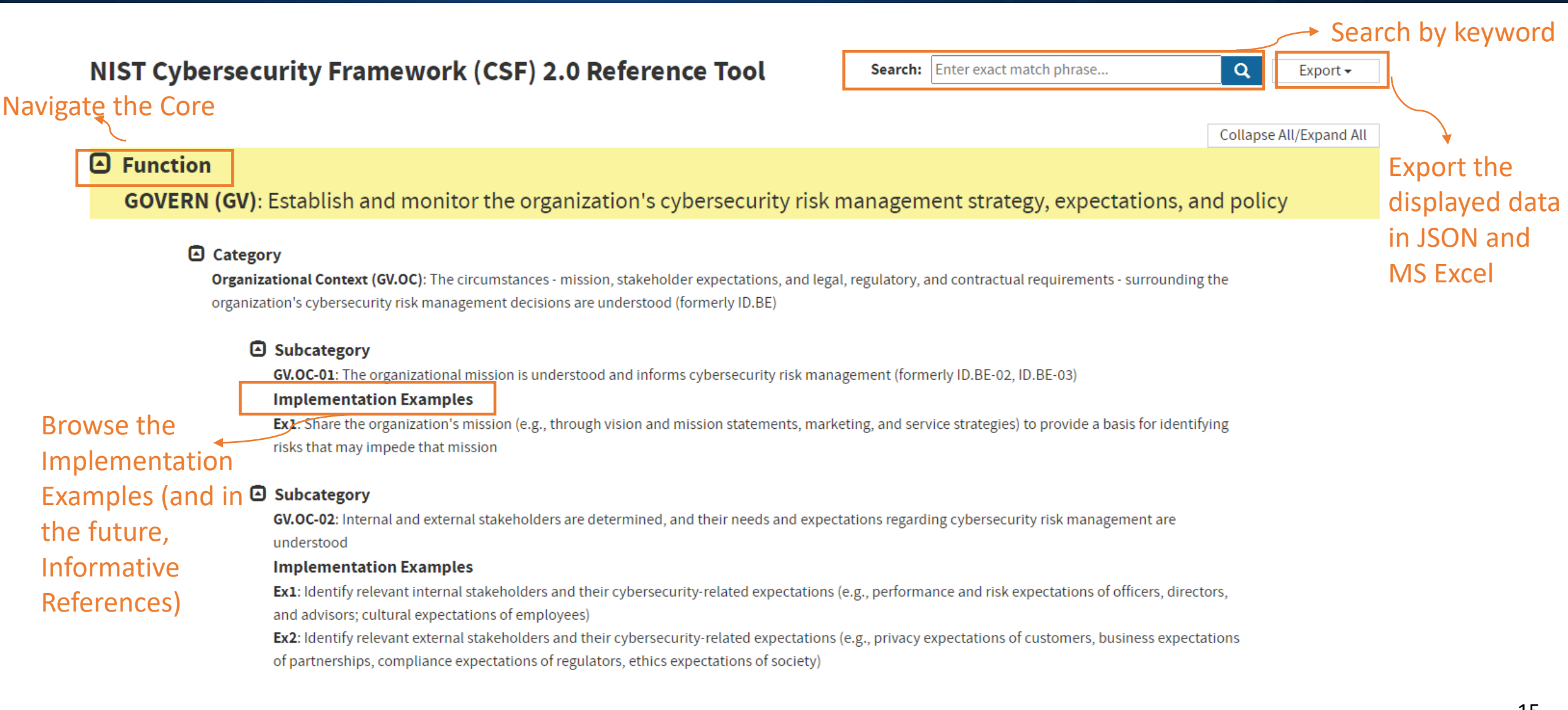
- Cyber Risk Institute: **The Profile (Financial Sector Profile)**
- FCC CSRIC: **Communications Sector Profile**
- NTCA: **Guide for Small Network Service Providers**
- Cybersecurity Coalition: **Botnet Threat Profile**
- Cybersecurity Coalition: **DDoS Threat Mitigation Profile**

All resources on NIST CSF website: www.nist.gov/cyberframework
Sample CSF Profiles: https://www.nist.gov/cyberframework/examples-framework-profiles

CSF Mappings – CPRT and OLIR



Cybersecurity Privacy Reference Tool (CPRT)



Examples of NCCoE Technology-Specific Mapping to the CSF

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Map the security capabilities demonstrated in each project to the CSF

Implementing a Zero Trust Architecture	*End-to-end zero trust architecture implementations to help industry and government reduce the risk of cyber attack*	*SP 1800-35E: Risk and Compliance Management (preliminary draft)*	ZTA security functions can help support the outcome described in the CSF subcategories
Supply Chain: Validating the Integrity of Computing Devices	*Helping organizations verify that the internal components of the computing devices they acquire are genuine and have not been tampered with*	*SP 1800-34B: Section 3.5 Security Control Map (final)*	The security characteristics can assist organizations better manage supply chain risk as expressed in CSF subcategories
		SP 1800-34B: Section 3.6 Technologies (final)	The specific products and services can help achieve the outcome described in the CSF subcategories
Trusted IoT Device Network-Layer Onboarding and Lifecycle Management	*Approaches to trusted network-layer onboarding of IoT devices and lifecycle management of the devices*	*Work in progress*	IoT on-boarding and security mechanisms security can help support the outcome described in the CSF subcategories
5G Cybersecurity	*Cybersecurity guidance to help consumers and operators of 5G networks securely adopt this technology as the development, deployment, and usage of 5G simultaneously evolves*	*Work in progress*	5G protocols and underlying infrastructure security mechanisms can help support the outcome described in the CSF subcategories
Migration to Post-Quantum Cryptography	*Initiating the development of practices to ease migration from the current set of public-key cryptographic algorithms to replacement algorithms that are resistant to quantum computer-based attacks*	*Work in progress*	Practices followed in preparation and during the migration can help support the outcome described in the CSF subcategories

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Thank You!

nccoe@nist.gov

nccoe.nist.gov

@NISTcyber