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

Resources to Help SMEs Manage Cybersecurity Risks When Doing Business in the Transatlantic Marketplace

June 26, 2024

This webinar is being recorded

Agenda

- Opening Remarks
- About NIST
- NIST International Engagement
- NIST Small Business Cybersecurity Resources
  - Small Business Cybersecurity Corner
  - CSF 2.0 Small business Quick Start Guide
  - Supply Chain Risk Management Quick Start Guide
- Overview of NIST Manufacturing Extension Partnership (MEP) ExporTech Program
- Audience Q&A

Opening Remarks

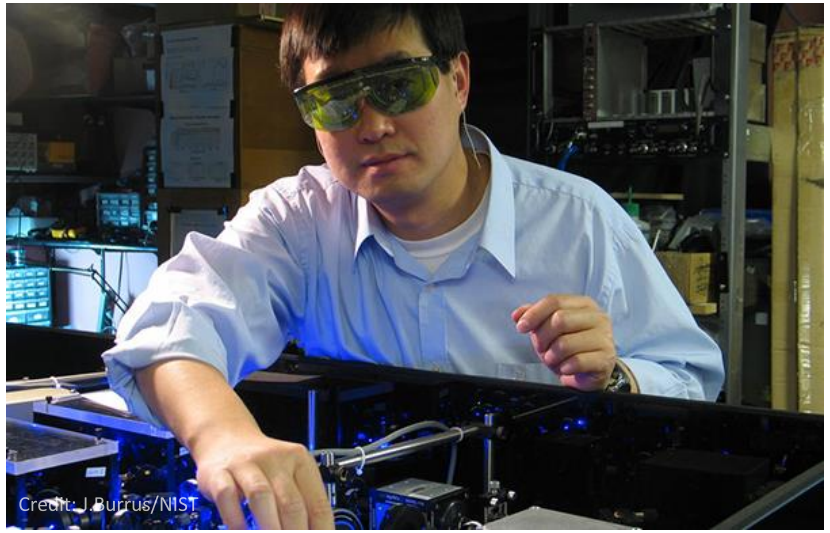
David De Falco

Deputy Assistant Secretary for Europe and Eurasia.
Global Markets, International Trade Administration,
United States Department of Commerce

This webinar supports the efforts of the U.S.-EU Trade and Technology Council (TTC) Working Group 9 to improve SME access to and use of digital tools. For more information about the TTC, please visit: https://www.trade.gov/useuttc

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



www.nist.gov

Celebrating 50+ Years of Cybersecurity

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

The Applied Cybersecurity Division **implements practical cybersecurity and privacy through outreach and effective application of standards and best practices** necessary for the U.S. to adopt cybersecurity capabilities.

https://www.nist.gov/itl/applied-cybersecurity

NIST International Engagement on Cybersecurity and Privacy Standards

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

International Engagement at NIST

- The cross-border nature of our economies makes it critical that NIST considers the global context when it conducts research, determines priorities, and conceptualizes approaches.
- As a result of widespread international use, there are now multiple translations and adaptations of NIST cybersecurity and privacy resources.
- NIST encourages international participation at all stages in the development and evolution of its cybersecurity and privacy programs and resources.

Learn About Our Global Impact: https://www.nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources

International Engagement on Resources

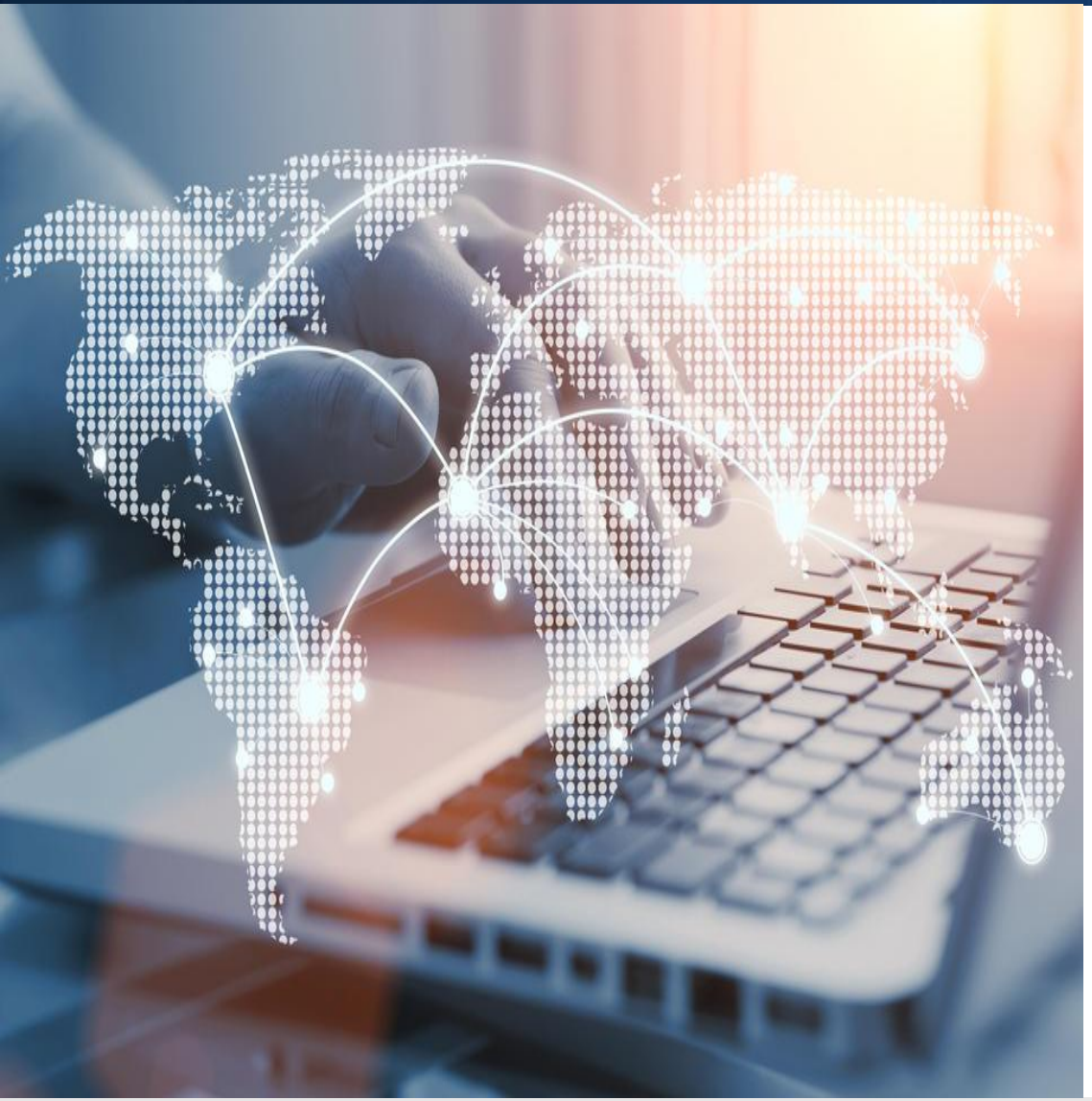
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

- The CSF and other NIST cybersecurity and privacy resources have benefitted from international expertise and are rooted in international standards.
- The CSF is currently used by government and industry in several countries and regions. Version 1.1 is translated into thirteen languages and Version 2.0 is currently translated into two languages.
- International engagement remains a focus for CSF 2.0.
- Work with interagency partners, including the State Department and International Trade Administration (ITA), to share information on NIST cybersecurity and privacy resources to international government partners.
- Work closely with industry on international engagements, including meetings, webinars, and side events during large international conferences.

Translations and adaptations of NIST resources are highlighted on the NIST International Cybersecurity and Privacy Resource Site:

https://www.nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources

Standards Activities in ISO



- NIST has contributed to the following documents in ISO that leverage the CSF:
  - ISO Technical Specification 27110, “Cybersecurity Framework Guidelines,” which specifies guidance for developing a cybersecurity framework that aligns with the functions of the CSF
  - ISO Technical Reference 27103, “Cybersecurity and ISO and IEC Standards,” which provides guidance on how to leverage existing ISO standards in a cybersecurity framework and maps to the CSF
- NIST is currently contributing as an editor on ISO 27028, a proposed international standard for guidance for attributes for the recently revised ISO 27002 standard

Learn About Our Global Impact: https://www.nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources

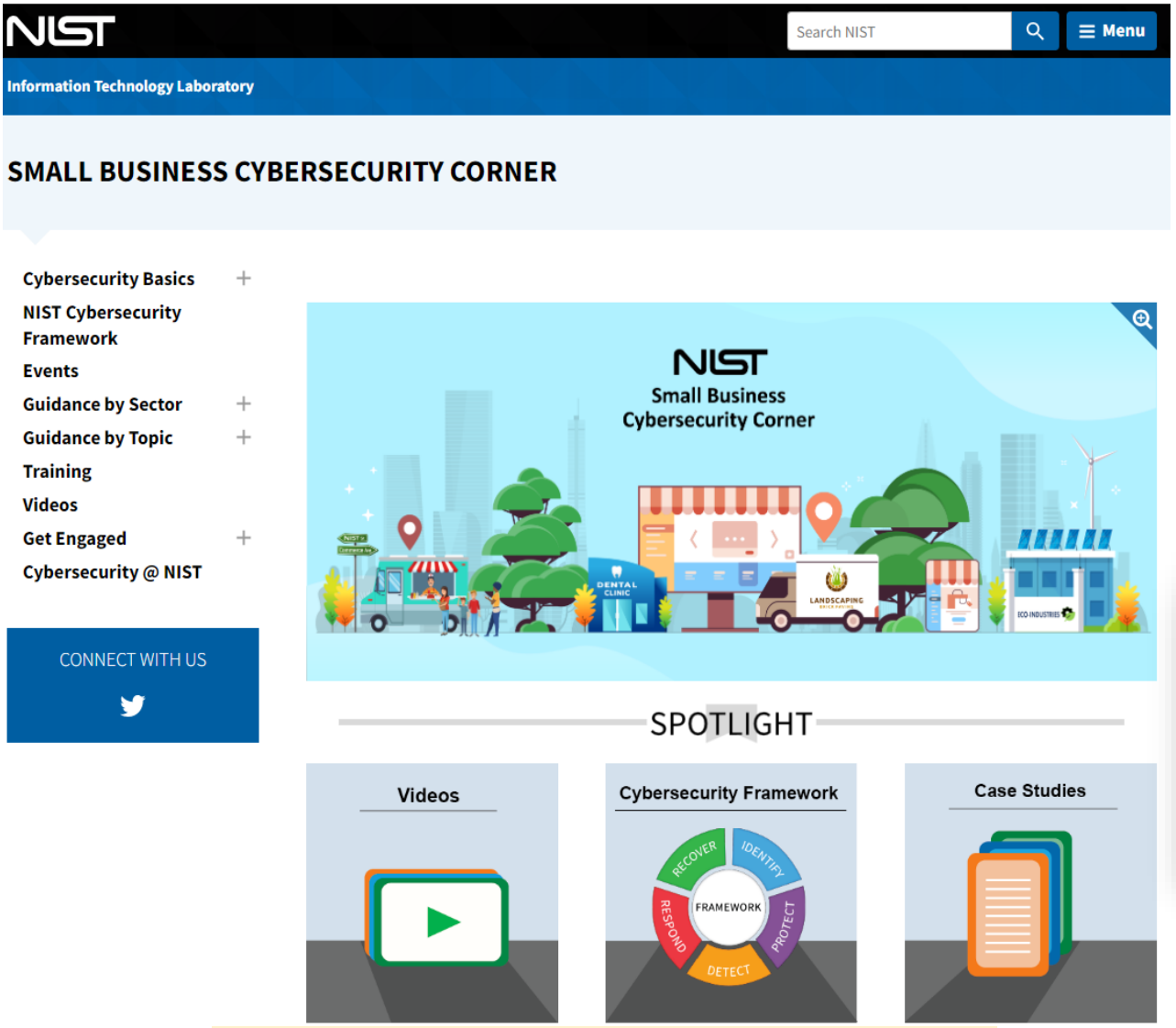
NIST Small Business Cybersecurity Resources

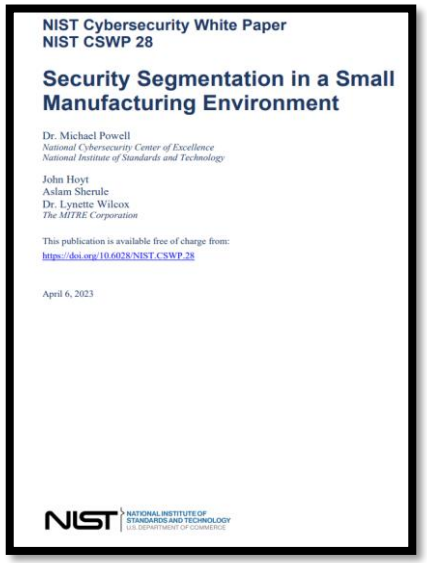
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

www.nist.gov/itl/smallbusinesscyber

NIST Small Business Cybersecurity Resources

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




NIST Cybersecurity White Paper
NIST CSWP 28

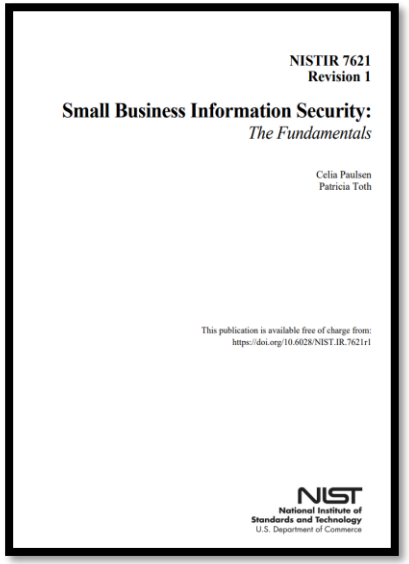
Security Segmentation in a Small Manufacturing Environment

Dr. Michael Powell
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

John Hoyt
Aslam Sherule
Dr. Lynette Wilcox
The MITRE Corporation

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.28

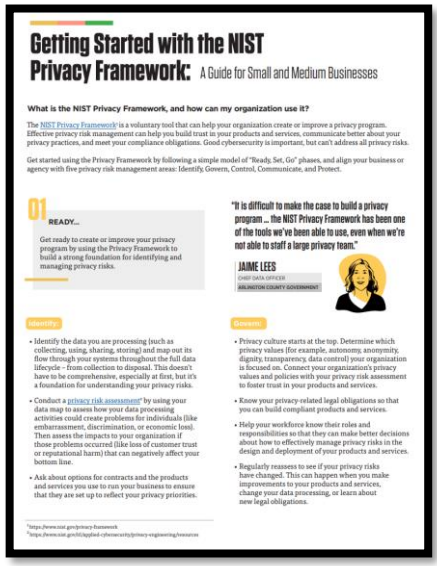
April 6, 2023


NISTIR 7621
Revision 1

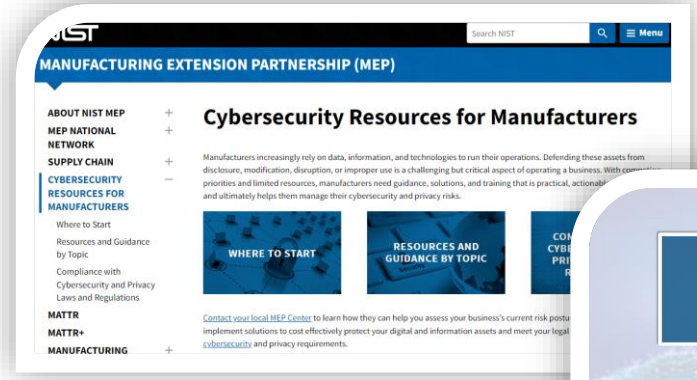
Small Business Information Security:
The Fundamentals

Celia Paulsen
Patricia Toth

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.7621r1


Getting Started with the NIST Privacy Framework: A Guide for Small and Medium Businesses

What is the NIST Privacy Framework, and how can my organization use it?



www.nist.gov/itl/smallbusinesscyber

NIST Small Business Cybersecurity Corner

https://www.nist.gov/itl/smallbusinesscyber

Guidance by Topic

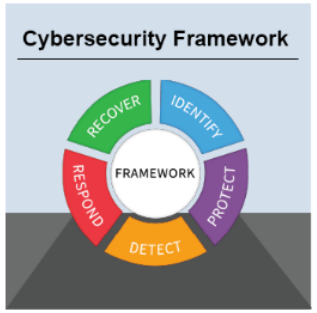
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

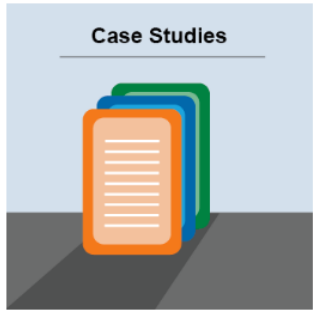
SMALL BUSINESS CYBERSECURITY CORNER

- Cybersecurity Basics
- NIST Cybersecurity Framework
- Events
- Guidance by Sector +
- Guidance by Topic +
- Training +
- Videos
- Get Engaged +
- Cybersecurity @ NIST

CONNECT WITH US

SPOTLIGHT

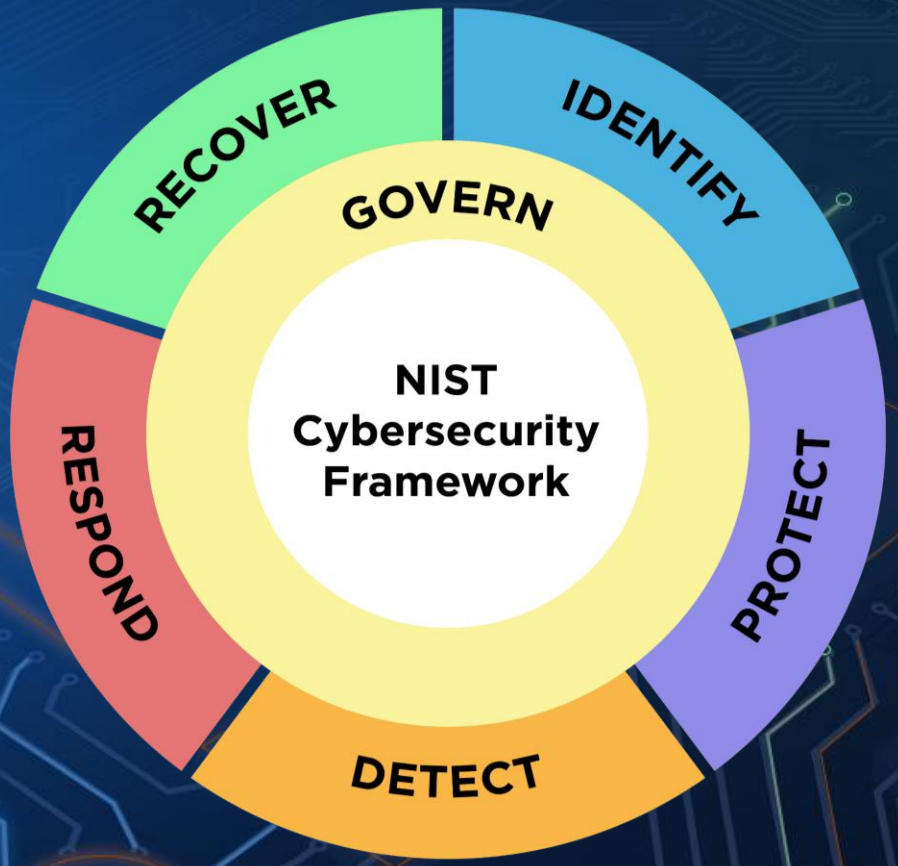




- ✓ All-Purpose Guides
- ✓ Choosing A Service Provider
- ✓ Cloud Security
- ✓ Cybersecurity Insurance
- ✓ Government Contractor Requirements
- ✓ Developing Secure Products
- ✓ Employee Awareness
- ✓ Multi-Factor Authentication
- ✓ Phishing
- ✓ Privacy
- ✓ Protecting Against Scams
- ✓ Ransomware
- ✓ Responding to a Cyber Incident
- ✓ Securing Data and Devices
- ✓ Securing Network Connections
- ✓ Telework

www.nist.gov/itl/smallbusinesscyber

CSF 2.0



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

https://www.nist.gov/cyberframework

NIST Cybersecurity Framework

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

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

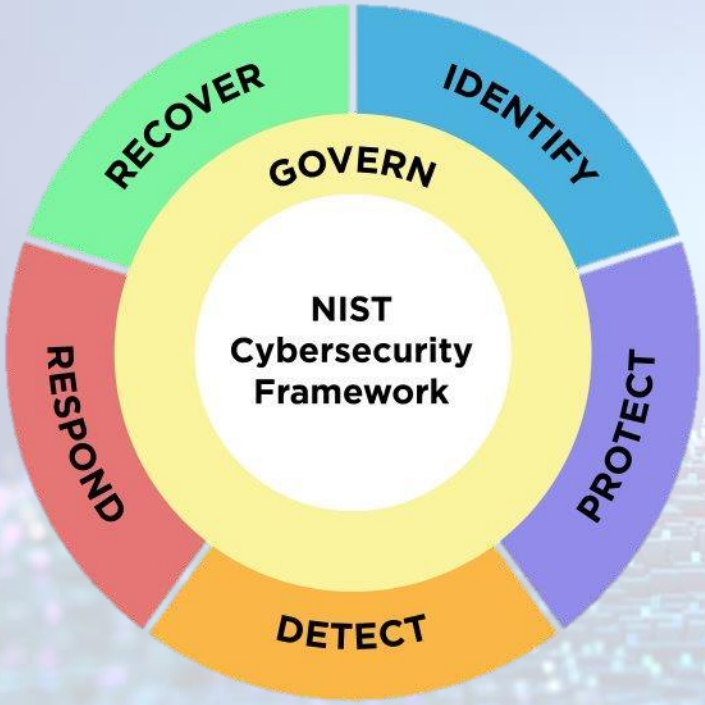
**not a one-size-fits-all approach to managing cybersecurity risks.*

CSF Core	CSF Organizational Profiles	CSF Tiers
The nucleus of the CSF. **A taxonomy of high-level cybersecurity outcomes** that can help any organization manage its cybersecurity risks. Functions>Categories>Subcategories	A mechanism for describing an organization's **current and/or target cybersecurity posture** in terms of the CSF Core's outcomes.	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.

https://www.nist.gov/cyberframework

NIST CSF 2.0 Small Business Quick Start Guide as an On-Ramp to the CSF 2.0 Journey

View full CSF 2.0 SMB QSG: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf



Together, these 6 Functions provide a comprehensive view for managing cybersecurity risk.

GOVERN

The Govern Function helps you establish and monitor your business's cybersecurity risk management strategy, expectations, and policy.

Actions to Consider

Understand

- Understand how cy *(GV.OC-01)*
- Understand your le
- Understand who w cybersecurity strate

Assess

- Assess the potentia operations. *(GV.OC-*
- Assess whether cyt
- Assess cybersecurit formal relationship

Prioritize

- Prioritize managing

Communicate

- Communicate lead culture. *(GV.RR-01)*
- Communicate, enfo

Getting Started with Cybersecurity Governance

You can use these tables to begin thinking about your cybersecurity governance strategy.

IDENTIFY

The Identify Function helps you determine the current cybersecurity risk to the business.

Actions to Consider

Understand

- Understand what inventory of hard

Assess

- Assess your asset
- Assess the effecti that need improv

Prioritize

- Prioritize inventor
- Prioritize docume responses using a

Communicate

- Communicate cyb relevant third par
- Communicate to cybersecurity risk

Getting Started with Identifying Current Cybersecurity Risk to Your Business

Before you can protect your assets, you need to identify them. Then you can determine the appropriate level of protection for each asset based upon its sensitivity and criticality to your

PROTECT

The Protect Function supports your ability to use safeguards to prevent or reduce cybersecurity risks.

Actions to Consider

Understand

- Understand what information employees should or do have access to. Restrict sensitive inform jobs. *(PR.AA-05*

Assess

- Assess the time training for emp

Prioritize

- Prioritize requir consider using protect strong
- Prioritize chang
- Prioritize regula Enable automat
- Prioritize regula
- Prioritize config protect data. *(P*

Communicate

- Communicate suspicious activ

Getting Started with Protecting Your Business

Enabling multi-factor authentication (MFA) is one of the fastest, cheapest ways you can protect your data. Start with accounts that can access the most sensitive information. Use this checklist to give you a head start, but remember your own list will be longer than this:

DETECT

The Detect Function provides outcomes that help you find and analyze possible cybersecurity attacks and compromises.

Actions to Consider

Understand

- Understand how *(DE.CM)*

Assess

- Assess your con expected or typ
- Assess your phy *(DE.CM-02)*

Prioritize

- Prioritize install business device
- Prioritize engag suspicious activ *(DE.CM)*

Communicate

- Communicate w the relevant det it. *(DE.AE-06/0*

Getting Started with Detecting Incidents

Some common indicators of a cybersecurity incident are:

- Loss of usual access to data, applications, or services

RESPOND

The Respond Function supports your ability to take action regarding a detected cybersecurity incident.

Actions to Consider

Understand

- Understand wha responsibility fo

Assess

- Assess your abil
- Assess the incid *(RS.AN-03, RS.M*

Prioritize

- Prioritize taking damage. *(RS.MI*

Communicate

- Communicate a stakeholders (e. regulatory bodi *(RS.CO-02/03)*

Getting Started with an Incident Response Plan

Before an incident occurs, you want to be ready with a basic response

Contact	Phone
Business Leader:	

RECOVER

The Recover Function involves activities to restore assets and operations that were impacted by a cybersecurity incident.

Actions to Consider

Understand

- Understand who within and outside your business has recovery responsibilities. *(RC.RP-01)*

Assess

- Assess what happened by preparing an after-action report—on your own or in consultation with a vendor/partner—that documents the incident, the response and recovery actions taken, and lessons learned. *(RC.RP-06)*
- Assess the integrity of your backed-up data and assets before using them for restoration. *(RC.RP-03)*

Prioritize

- Prioritize your recovery actions based on organizational needs, resources, and assets impacted. *(RC.RP-02)*

Communicate

- Communicate regularly and securely with internal and external stakeholders. *(RC.CO)*
- Communicate and document completion of the incident and resumption of normal activities. *(RC.RP-06)*

Getting Started with a Recovery Playbook

A playbook typically includes the following critical elements:

- ✓ A set of formal recovery processes
- ✓ Documentation of the criticality of organizational resources (e.g., people, facilities, technical components, external services)
- ✓ Documentation of systems that process and store organizational information, particularly key assets. This will help inform the order of restoration priority
- ✓ A list of personnel who will be responsible for defining and implementing recovery plans
- ✓ A comprehensive recovery communications plan

Technical Deep Dive: NIST Guide for Cybersecurity Event Recovery

Questions to Consider

- What are our lessons learned? How can we minimize the chances of a cybersecurity incident happening in the future?
- What are our legal, regulatory, and contractual obligations for communicating to internal and external stakeholders about a cybersecurity incident?
- How do we ensure that the recovery steps we are taking are not introducing new vulnerabilities to our business?

Related Resources

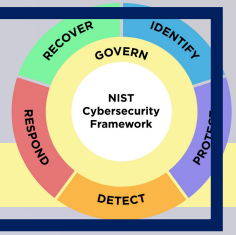
- Cybersecurity Training Resources
- Creating an IT Disaster Recovery Plan
- Backup and Recover Resources

View all NIST CSF 2.0 Resources Here

https://www.nist.gov/cyberframework

GOVERN

The Govern Function helps you establish and monitor your business's cybersecurity risk management strategy, expectations, and policy.



Actions to Consider

Understand

- Understand how cybersecurity r
  (GV.OC-01
- Understand your legal, regulato
- Understand who within your bu
  cybersecurity strategy. *(GV.RR-0*

GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored

- **Organizational Context (GV.OC):** The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood
  - **GV.OC-01:** The organizational mission is understood and informs cybersecurity risk management

Assess

- Assess the potential impact of a total or partial loss of critical business assets and operations. *(GV.0C-04)*
- Assess whether cybersecurity insurance is appropriate for your business. *(GV.RM-04)*
- Assess cybersecurity risks posed by suppliers and other third parties before entering into formal relationships. *(GV.SC-06)*

Prioritize

- Prioritize managing cybersecurity risks alongside other business risks. *(GV.RM-03)*

Communicate

- Communicate leadership's support of a risk-aware, ethical, and continually improving culture. *(GV.RR-01)*
- Communicate, enforce, and maintain policies for managing cybersecurity risks. *(GV.PO-01)*

Getting Started with Cybersecurity Governance

Y es to begin thinking about your cybersecurity governance strategy.

nal Context	
n	
risks achieving this mission?	

Documenting Cybersecurity Requirements	
List your legal requirements:	
List your regulatory requirements:	
List your contractual requirements:	

Technical Deep Dive: Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight

Questions to Consider

- As our business grows, how often are we reviewing our cybersecurity strategy?
- Do we need to upskill our existing staff, hire talent, or engage an external partner to help us establish and manage our cybersecurity plan?
- Do we have acceptable use policies in place for business and for employee-owned devices accessing business resources? Have employees been educated on these policies?

Related Resources

- Securing Small and Medium-Sized Supply Chains Resource Handbook
- Choosing A Vendor/Service Provider

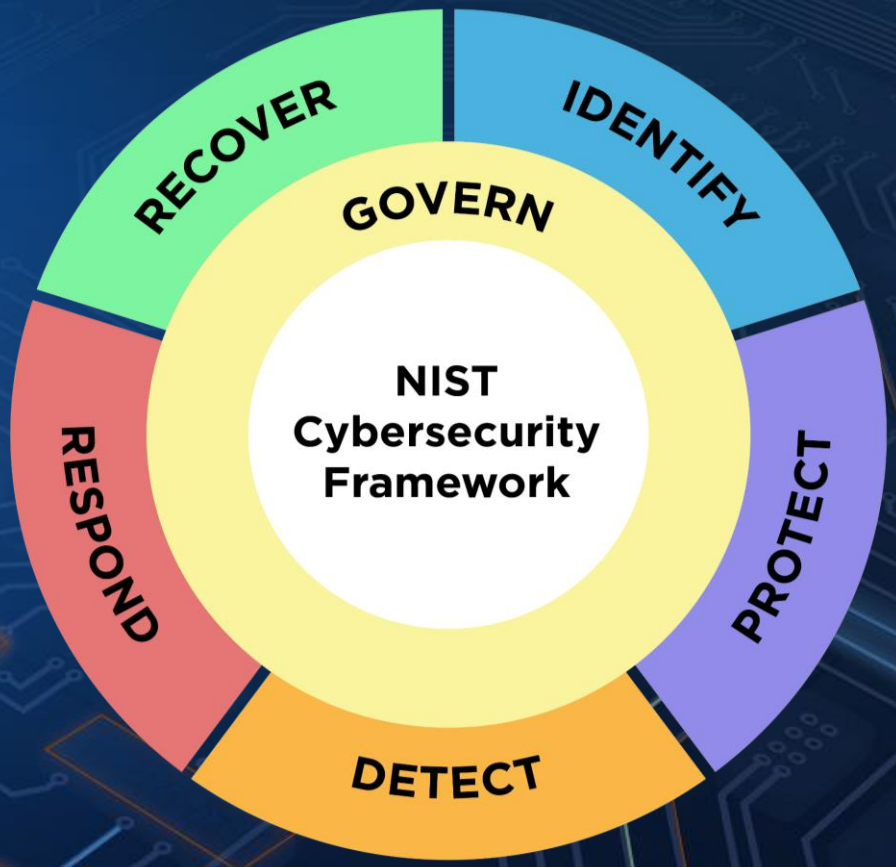
View all NIST CSF 2.0 Resources Here

A Few Notes on the Govern Function

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

- The Big Picture
- **Provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions**.
- Encompasses how organizations make and carry out **informed decisions** on cybersecurity strategy.
- Emphasizes that cybersecurity is a major source of enterprise risk that business leaders should consider alongside other business risks.
- Emphasis on supply chain risk management.

CSF 2.0 Cybersecurity Supply Chain risk Management (C-SCRM) Quick Start Guide



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

https://www.nist.gov/quick-start-guides

CSF 2.0 C-SCRM Quick Start Guide

https://www.nist.gov/quick-start-guides

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

NIST CSF 2.0: CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM)

A QUICK START GUIDE

HOW TO USE THE CSF TO ESTABLISH AND OPERATE A C-SCRM CAPABILITY

Establishing a C-SCRM Capability

The CSF has a Category within its Govern Function dedicated to C-SCRM: the Cybersecurity Supply Chain Risk Management (GV.SC) Category. GV.SC contains the key outcomes that every organization should achieve through its C-SCRM capability. Additionally, many of the subcategories within the remainder of the CSF can be used to identify and communicate C-SCRM-related requirements internally for organizations and for their vendors.

Perform these activities to establish your organization's C-SCRM capability:

Activity 1: Create a C-SCRM strategy, objectives, policies, and processes. [GV.SC-01]

Activity 2: Identify your organization's technology suppliers and determine how critical each one is to your organization. [GV.SC-04]

Activity 3: Establish C-SCRM roles and requirements and communicate them within and outside your organization. This includes identifying C-SCRM roles and responsibilities [GV.SC-02] and C-SCRM requirements [GV.SC-05].

It is also important to coordinate and harmonize activities between your C-SCRM capability and other internal capabilities. Here are a few examples:

- Integrate C-SCRM into cybersecurity and enterprise risk management, risk assessment, and improvement processes, and monitor the performance of C-SCRM practices throughout the technology lifecycle. [GV.SC-03, GV.SC-09] See the *Enterprise Risk Management Quick-Start Guide* for more information on C-SCRM integration.
- Include your relevant suppliers in cybersecurity incident planning, response, and recovery activities. [GV.SC-08] See NIST's *Computer Security Incident Handling Guide* for more information on key practices for cybersecurity incidents.

Checklist of actions for Activity 1: Create a C-SCRM strategy, objectives, policies, and processes.

- ☐ Establish a C-SCRM strategy that lays out the objectives of the capability.
- ☐ Develop a C-SCRM plan (with milestones) and C-SCRM policies and procedures that guide implementation and improvement of the plan and the capability; socialize those policies and procedures with organizational stakeholders.
- ☐ Develop and implement C-SCRM processes based on the strategy, objectives, policies, and procedures that are agreed upon and performed by the organizational stakeholders.
- ☐ Establish a cross-organizational mechanism that ensures alignment between functions that contribute to C-SCRM management, such as cybersecurity, IT, legal, human resources, engineering, etc.

Checklist of actions for Activity 2: Identify your organization's technology suppliers and determine how critical each one is to your organization.

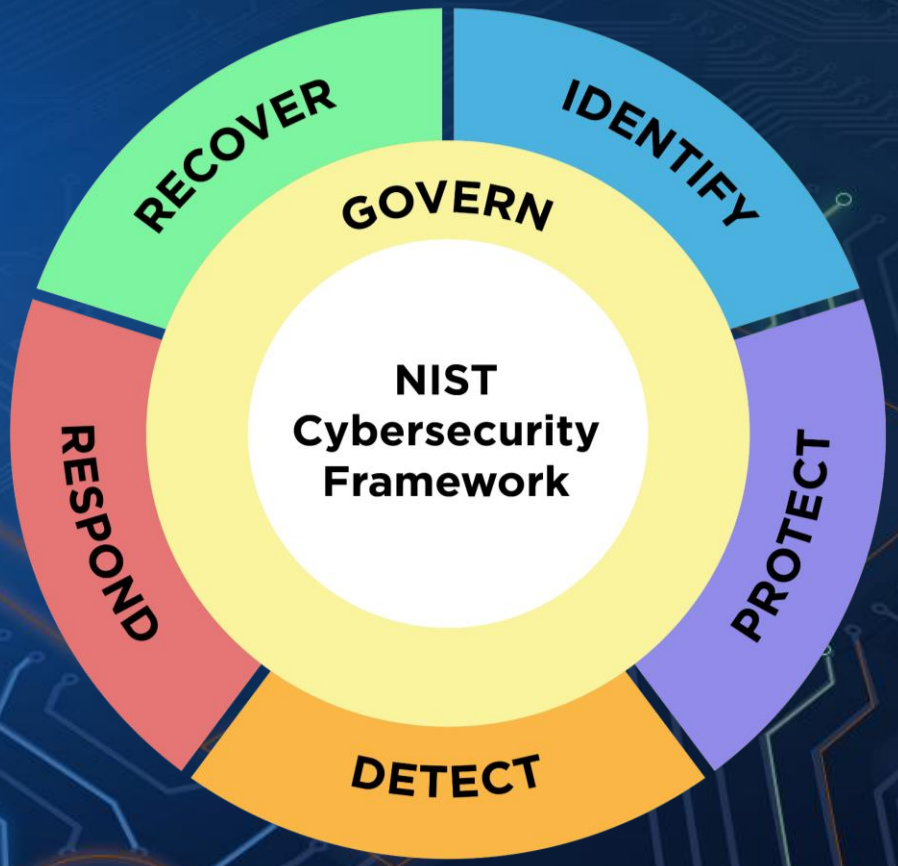
- ☐ Develop criteria for supplier criticality based on, for example, the importance of the supplier's products or services to the organization's business, sensitivity of data processed or stored by the supplier, and degree of access to the organization's systems.
- ☐ Prioritize suppliers into criticality levels based on the criteria. See NIST IR 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components* for more information on a structured method for prioritization.
- ☐ Keep a record of all suppliers, prioritized based on the criticality criteria.

New to C-SCRM?

Here are some NIST resources that can help you get up to speed on the basics of C-SCRM and support you in establishing and operating your C-SCRM capability:

- **CSF 2.0 C-SCRM Quick Start Guide**
  https://www.nist.gov/quick-start-guides
- **Key Practices in Cyber Supply Chain Risk Management: Observations from Industry (NIST IR 8276)**
  https://csrc.nist.gov/pubs/ir/8276/final
- **Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST SP 800-161 Revision 1)**
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf
- **The Software and Supply Chain Assurance Forum**
  https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/ssca
- **NIST's C-SCRM Program**
  https://csrc.nist.gov/projects/cyber-supply-chain-risk-management

Additional CSF 2.0 Resources

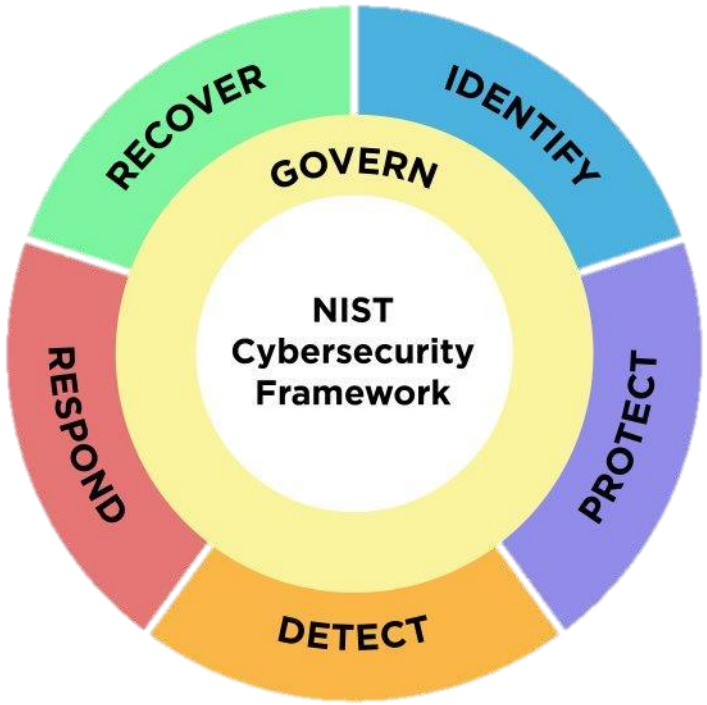


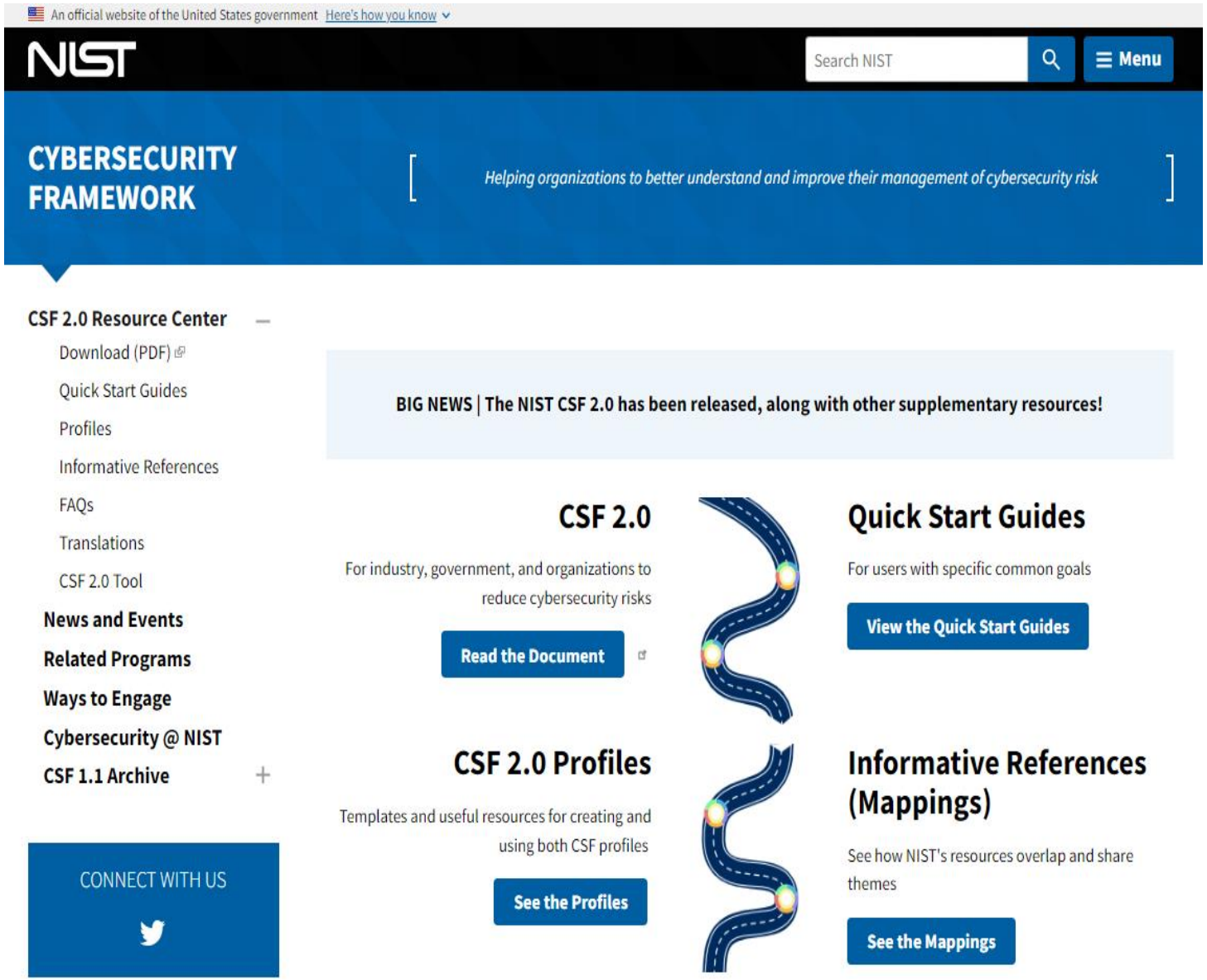
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

https://www.nist.gov/cyberframework

NIST.gov/cyberframework

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





Cybersecurity Framework 2.0 Reference Tool

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

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

The NIST Cybersecurity Framework 2.0
www.nist.gov/cyberframework

Function	Category	Subcategory	Implementation Examples	Informative References
GOVERN (GV)				
IDENTIFY (ID): The organization's current cybersecurity risks are understood				
	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			
		ID.AM-01: Inventories of hardware managed by the organization are maintained	Ex1: Maintain inventories for all types o hardware, including IT, IoT, OT, and mobile devices Ex2: Constantly monitor networks to detect new hardware and automatically update inventories	CIS Controls v8.0: 1.1 SP 800-53 Rev 5.1.1: CM-08 SP 800-53 Rev 5.1.1: PM-05
		ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	Ex1: Maintain inventories for all types o 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	CIS Controls v8.0: 2.1 SP 800-53 Rev 5.1.1: AC-20 SP 800-53 Rev 5.1.1: CM-08 SP 800-53 Rev 5.1.1: PM-05 SP 800-53 Rev 5.1.1: SA-05 SP 800-53 Rev 5.1.1: SA-09
		ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained	Ex1: Maintain baselines of communication and data flows within the organization's wired and wireless networks Ex2: Maintain baselines of communication and data flows betwee the organization and third parties Ex3: Maintain baselines of communication and data flows for the organization's infrastructure-as-a-servic (IaaS) usage Ex4: Maintain documentation of expected network ports, protocols, and	CIS Controls v8.0: 3.8 SP 800-53 Rev 5.1.1: AC-04 SP 800-53 Rev 5.1.1: CA-03 SP 800-53 Rev 5.1.1: CA-09 SP 800-53 Rev 5.1.1: PL-02 SP 800-53 Rev 5.1.1: PL-08 SP 800-53 Rev 5.1.1: PM-07
		ID.AM-04: Inventories of services provided by suppliers are maintained	Ex1: Inventory all external services used by the organization, including third-part infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) offerings; APIs; and other externally hosted application services	CIS Controls v8.0: 15.1 SP 800-53 Rev 5.1.1: AC-20 SP 800-53 Rev 5.1.1: SA-09 SP 800-53 Rev 5.1.1: SR-02

ExporTech – Accelerating sales growth in global markets for small and medium-sized manufacturers

NIST MANUFACTURING EXTENSION PARTNERSHIP

https://www.nist.gov/mep/mep-national-network

MEP National Network™

A unique public-private partnership that delivers comprehensive, proven solutions to U.S. manufacturers, fueling growth and advancing U.S. manufacturing.

Our mission is to strengthen and empower U.S. manufacturers.

MEP National Network

Centers located in all 50 states and Puerto Rico.

Public-private partnership with local flexibility.

Federal funds, state investments, and private sector fees cover services.

Market driven program that creates high value for manufacturers.

Leverage partners to maximize service offerings.

Transfer technology and expertise to manufacturers.

Business Solution Examples

ExporTech is a structured process that helps exporters expand sales in global markets

PLAN	• Develop strategic export growth plan through workshops, planning tools, and individual coaching • Receive plan feedback from experienced international business leaders
EDUCATE	• Learn from wide range of experts – with opportunity for individualized consultation
CONNECT	• Companies meet experts that become part of their network • Learn about programs, services, and grants that many exporters are unaware of • Learn from peer companies – and hold each other accountable
IMPLEMENT	• Execute plan, and connect to resources that can help you go-to-market (e.g. partner search and matchmaking, STEP grants, tradeshows) • Achieve higher ROI on business development – guided by plan

ExporTech Program Partners

Exporters

Local Partners
(differ by region)

- District Export Councils
- State trade offices/organizations
- FedEx
- Universities, colleges
- SBDCs, SBA offices
- World Trade Centers
- Private consultants
- State and federal department of agriculture
- Other economic development organizations
- City governments

MEP National Network

- Delivery
- Selling, marketing
- Program management

U.S. Commercial Service

- Delivery
- Selling, marketing
- Program management

Principles/Philosophy of ExporTech

- Aimed at leadership
- Each company develops strategic international growth plan, receives feedback for go-to-market strategy
- Customized to participants
- Highly interactive – breakouts, one-on-ones, speed dating

ExporTech Unique Elements

- Development of export plan with feedback in final session
- Breakout groups working on elevator pitch
- Coaching in between sessions
- Connection to export ecosystem – expand network
- Significant involvement of experienced exporting company executives (plan feedback, panel discussions, breakout consultations)

ExporTech National Program History and Impacts

Program Summary (6/20/24)

# Programs Completed (since inception in 2007)	275
# States	37 (and PR)
# Participating Companies	1,380

EXPORTECH™
An Export Acceleration System for Achieving Profitable Growth

Client Impact

- Average sales increase/retention of **$469,000**
- Average cost savings of **$93,000**
- Average **6** new jobs per company
- Total program impact to date: >**$600 million** sales increase/retention

Success Story

Hydronalix Grows Export Markets Fivefold in Five Years

- Manufactures robotic water rescue systems and small unmanned watercraft in Green Valley, Arizona.
- First responders and military use: water rescue, bridge inspection, scientific research and law enforcement on oceans, lakes, and rivers.
- *The Challenge:* selling into export markets but no defined strategy/process.
- ExporTech partners helped company develop an export plan - how to structure and negotiate payment terms to ensure up-front payment.
- Executed export plan through international trade shows and trade mission initiatives led by the AZSTEP program - met with potential sales channel partners, end-users and buyers.

*"I think the success of the program is because it's been **repeatable and sustainable**. It takes a lot of continuous effort to grow our global customer base. In our case, ExporTech provided that critical push. In 2016, before we started ExporTech, I think we were selling in 11 or 12 countries. Now we have distributors in **33 countries, and we sell our products in 50 countries.** The program has had a big impact on our business."*

Hydronalix CEO

Connect with Us

Visit Our Blog

www.nist.gov/blogs/manufacturing-innovation-blog

Visit Our Website

www.nist.gov/mep

www.nist.gov/exportech

Contact Us:

Brian.Lagas@nist.gov

301-975-5043

Quick Links	Contact Information
CSF 2.0 Website: https://www.nist.gov/cyberframework **CSF 2.0 FAQs:** https://www.nist.gov/faqs	cyberframework@nist.gov
CSF 2.0 Small Business Quick Start Guide: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf **NIST Small Business Cybersecurity Corner:** https://www.nist.gov/itl/smallbusinesscyber	smallbizsecurity@nist.gov
CSF 2.0 C-SCRM Quick Start Guide: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1305.ipd.pdf	scrm-nist@nist.gov
Cybersecurity and Privacy Reference Tool (CPRT): https://csrc.nist.gov/Projects/cprt	cprt@nist.gov
NIST International Cybersecurity and Privacy Resources: https://www.nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources	intl-cyber-privacy@nist.gov
Computer Security Resource Center: https://csrc.nist.gov/publications	csrc-inquiry@nist.gov
EXPORTECH https://www.nist.gov/exportech	Brian.Lagas@nist.gov


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