Overview of the NIST Cybersecurity Framework (CSF) 2.0 Small Business Quick Start Guide

March 20, 2024

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

This webinar is being recorded

Submitting Questions

Please use the Q&A window to enter your questions.

1. To open the Q&A panel, click on the ellipses at the bottom of the screen for 'More Panels' and click on Q&A.

2. Type your question in the text box and click Send

This webinar is being recorded

Agenda

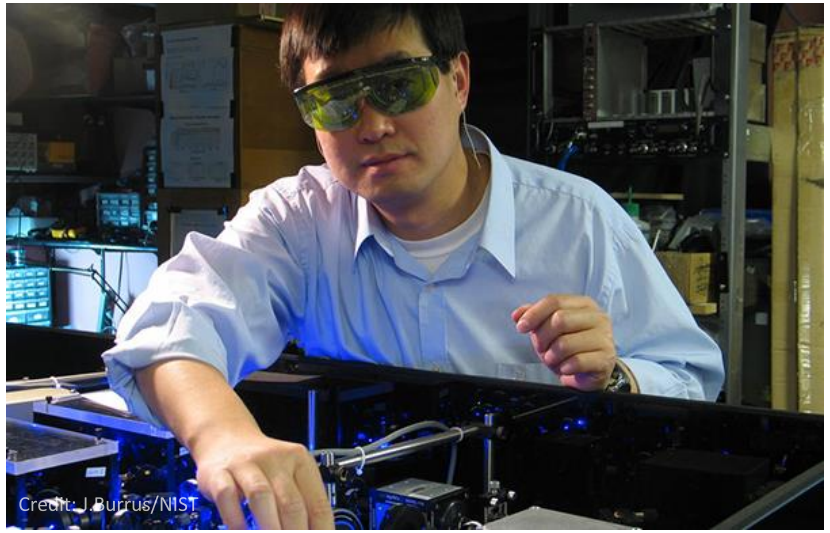
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

- Introduction
- Brief Overview of CSF 2.0
- Overview of the CSF 2.0 Small Business Quick Start Guide
- Additional CSF 2.0 Resources
- Getting Engaged with NIST Small Business Cybersecurity Efforts
- Q&A

This webinar is being recorded

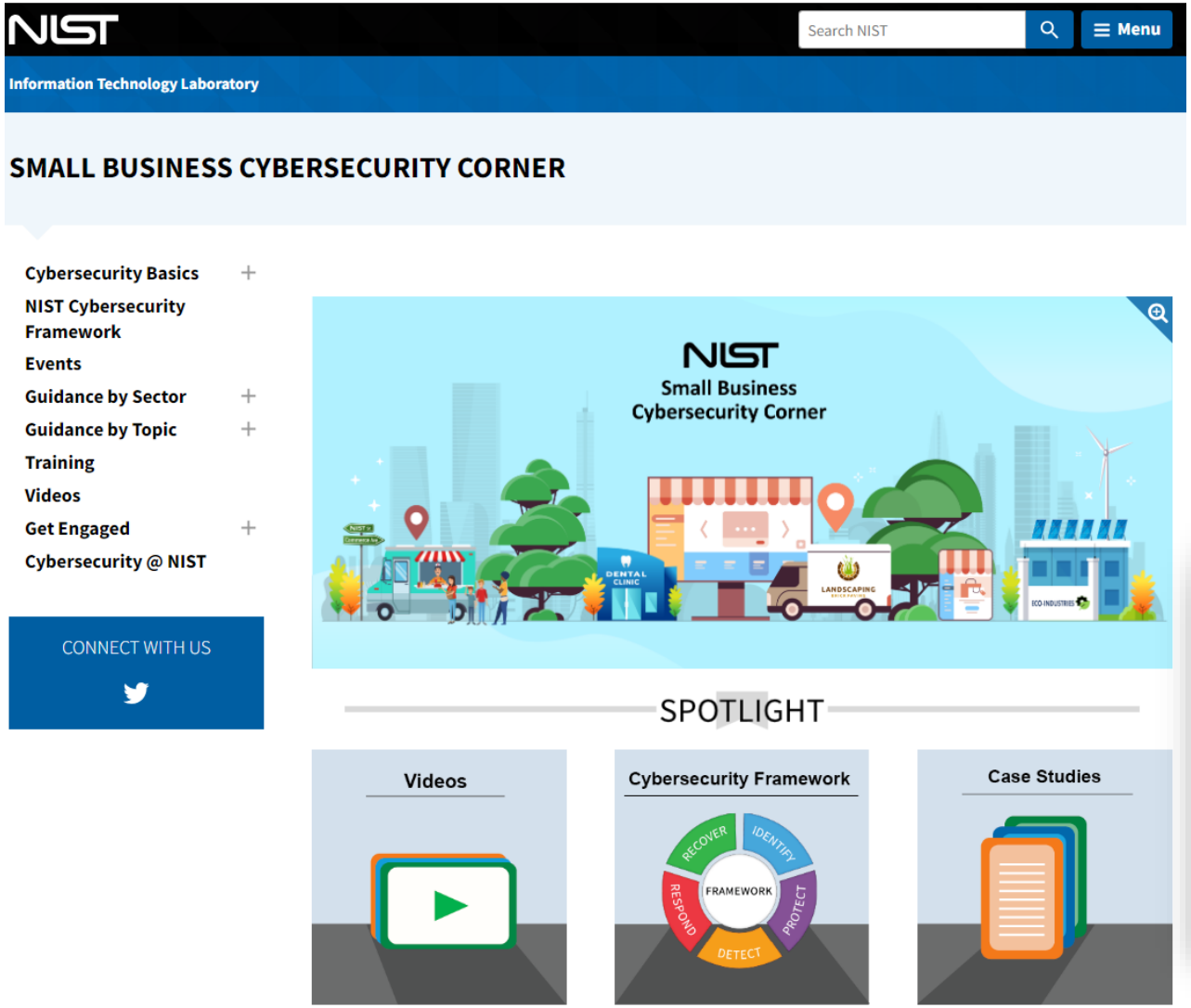
NIST Mission

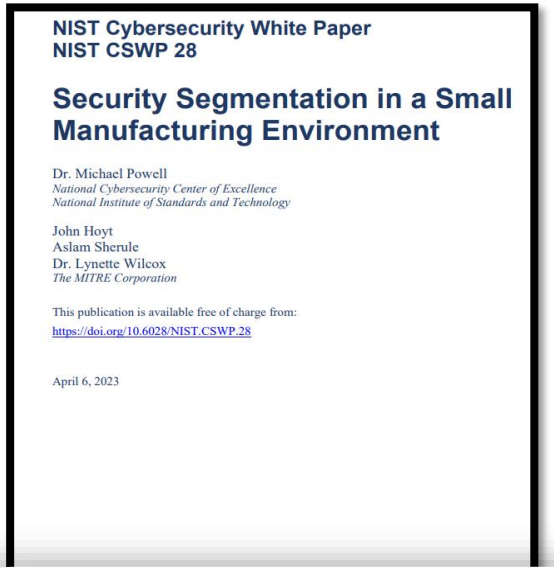
To promote U.S. innovation and industrial competitiveness by advancing **measurement science, standards, and technology** in ways that enhance economic security and improve our quality of life

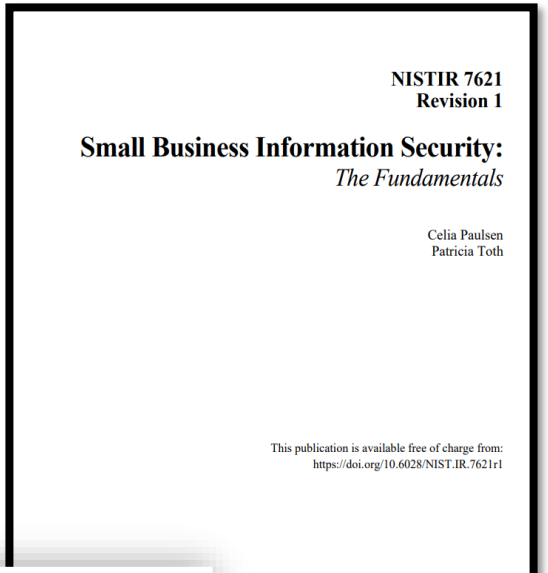


NIST Small Business Cybersecurity Resources

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

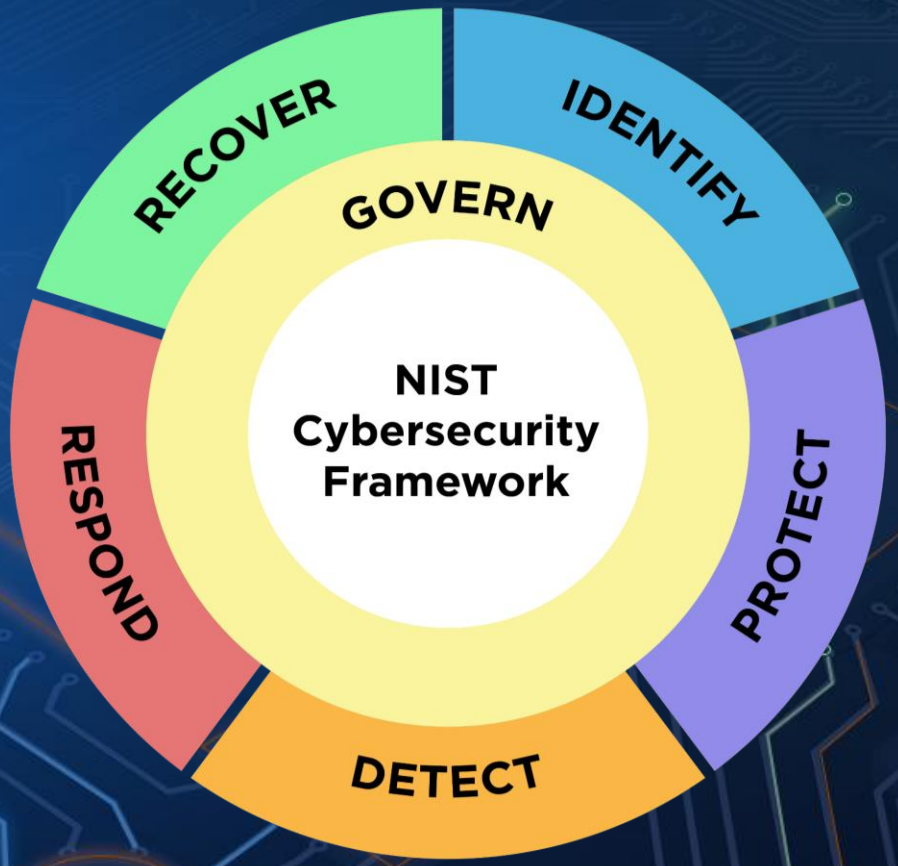






www.nist.gov/itl/smallbusinesscyber

Brief Overview of CSF 2.0



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

https://www.nist.gov/cyberframework

CSF 2.0 | What Makes it Different?

- ✓ Expanded scope beyond critical infrastructure
- ✓ Addition of a 6th Core Function “Govern”
- ✓ Increased emphasis on supply chain risk management
- ✓ We listened to your feedback, made key updates, **developed new resources and tools**, and adjusted our guidance based on today’s cybersecurity environment.

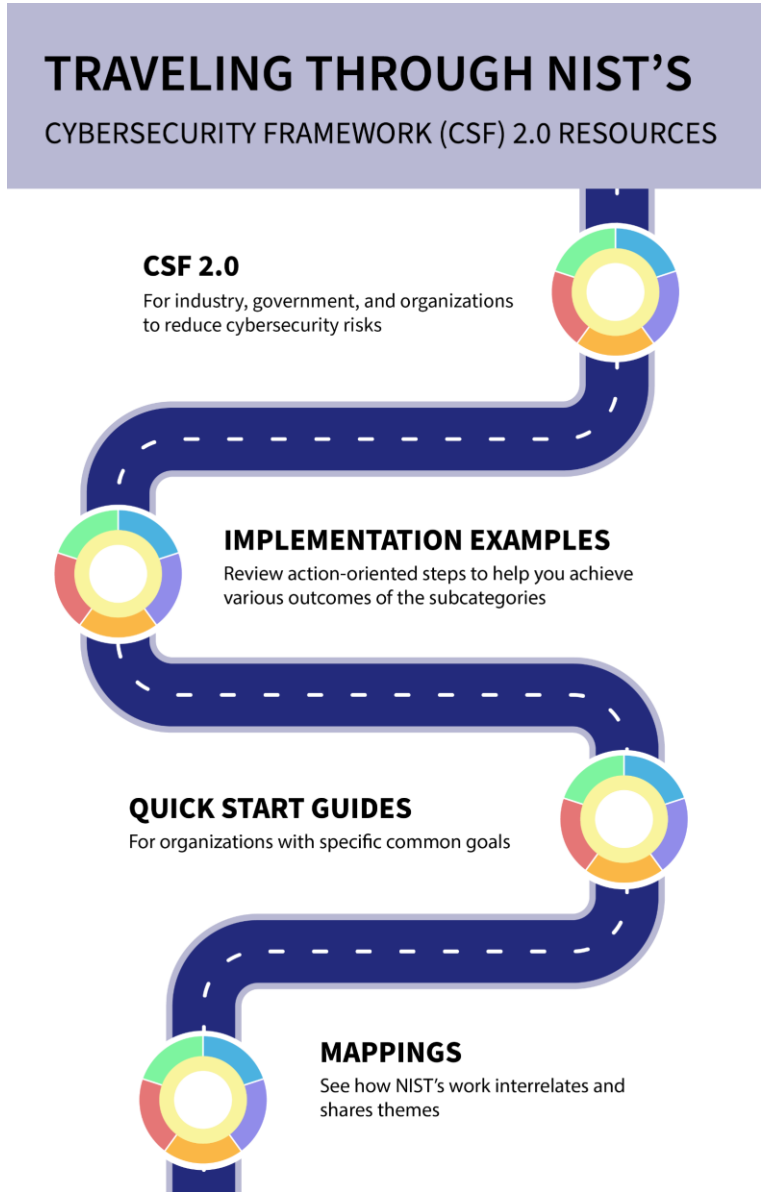
Resources Showing Differences Between CSF 1.1 and CSF 2.0:

NIST Cybersecurity Framework 2.0 Reference Tool- https://csrc.nist.gov/extensions/nudp/services/json/csf/download?olirids=all

From the CSF 2.0 Tool page - CSF 2.0 Reference Tool

The Crosswalk from the OLIR catalog with more detail - https://csrc.nist.gov/csrc/media/Projects/olir/documents/submissions/CSFv1.1_to_CSFv2.0_CROSSWALK_20240220.xlsx

View all CSF 2.0 FAQS: https://www.nist.gov/faqs



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

Creation of CSF 2.0 SMB QSG

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

- There was a clear desire for an actionable, accessible small business-focused CSF resource.
- Leveraging Implementation Examples as content for “Actions to Consider.”
- Focus on usability and readability.
- Focus on a limited number of high priority items that an under-resourced organization can implement.
- Thank you to the America’s Small Business Development Cybersecurity Task Force for your feedback and review.
- Creation of something that can start a dialogue.

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

IDENTIFY

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

Actions to Consider

Understand

- Understand what assets your business relies upon by creating and maintaining an inventory of hardware, software, systems, and services. *(ID.AM-01/02/04)*

Assess

- Assess your assets (IT and physical) for potential vulnerabilities. *(ID.RA-01)*
- Assess the effectiveness of the business's cybersecurity program to identify areas that need improvement. *(ID.IM-01)*

Prioritize

- Prioritize inventorying and classifying your business data. *(ID.AM-07)*
- Prioritize documenting internal and external cybersecurity threats and associated responses using a risk register. *(ID.RA)*

Communicate

- Communicate cybersecurity plans, policies, and best practices to all staff and relevant third parties. *(ID.IM-04)*
- Communicate to staff the importance of identifying needed improvements to cybersecurity risk management processes, procedures, and activities. *(ID.IM)*

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 business mission. You can use this sample table to get started on your information technology (IT) asset inventory. As your business matures, you might consider using an automated asset inventory solution or a managed security service provider to help you manage all your business assets.

Software/ hardware/ system/ service	Asset's official use:	Asset administrator or owner:	Identify sensitive data the asset has access to:	Is multi-factor authentication required to access this asset?	Risk to business if we lose access to this asset

Technical Deep Dive: Integrating Cybersecurity and Enterprise Risk Management

Questions to Consider

- What are our most critical business assets (data, hardware, software, systems, facilities, services, people, etc.) we need to protect?
- What are the cybersecurity and privacy risks associated with each asset?
- What technologies or services are personnel using to accomplish their work? Are these services or technologies secure and approved for use?

Related Resources

- NIST Risk Register Template
- Take Stock. Know What Sensitive Information You Have
- Evaluating Your Operational Resilience and Cybersecurity Practices

View all NIST CSF 2.0 Resources Here

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 information access to only those employees who need it to do their jobs. *(PR.AA-05)*

Assess

- Assess the timeliness, quality, and frequency of your company's cybersecurity training for employees. *(PR.AT-01/02)*

Prioritize

- Prioritize requiring multi-factor authentication on all accounts that offer it and consider using password managers to help you and your staff generate and protect strong passwords. *(PR.AA-03)*
- Prioritize changing default manufacturer passwords. *(PR.AA-01)*
- Prioritize regularly updating and patching software and operating systems. Enable automatic updates to help you remember. *(PR.PS-02)*
- Prioritize regularly backing up your data and testing your backups. *(PR.DS-11)*
- Prioritize configuring your tablets and laptops to enable full-disk encryption to protect data. *(PR.DS-01)*

Communicate

- Communicate to your staff how to recognize common attacks, report attacks or suspicious activity, and perform basic cyber hygiene tasks. *(PR.AT-01/02)*

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:

Account	MFA Enabled (Y/N)
Banking Account(s)	
Accounting and Tax Account(s)	
Merchant Account(s)	
Google, Microsoft, and/or Apple ID Account(s)	
Email Account(s)	
Password Manager(s)	
Website Account(s)	

Technical Deep Dive: NIST Digital Identity Guidelines

Questions to Consider

- Are we restricting access and privileges only to those who need it? Are we removing access when they no longer need it?
- How are we securely sanitizing and destroying data and data storage devices when they're no longer needed?
- Do employees possess the knowledge and skills to perform their jobs with security in mind?

Related Resources

- Cybersecurity Training Resources
- Multi-Factor Authentication
- Protecting Your Business from Phishing

View all NIST CSF 2.0 Resources Here

DETECT

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

Actions to Consider

Understand

- Understand how to identify common indicators of a cybersecurity incident. *(DE.CM)*

Assess

- Assess your computing technologies and external services for deviations from expected or typical behavior. *(DE.CM-06/09)*
- Assess your physical environment for signs of tampering or suspicious activity. *(DE.CM-02)*

Prioritize

- Prioritize installing and maintaining antivirus and anti-malware software on all business devices—including servers, desktops and laptops. *(DE.CM-09)*
- Prioritize engaging a service provider to monitor computers and networks for suspicious activity if you don't have the resources to do it internally. *(DE.CM)*

Communicate

- Communicate with your authorized incident responder, such as an MSSP, about the relevant details from the incident to help them analyze and mitigate it. *(DE.AE-06/07)*

Getting Started with Detecting Incidents

Some common indicators of a cybersecurity incident are:

- Loss of usual access to data, applications, or services
- Unusually sluggish network
- Antivirus software alerts when it detects that a host is infected with malware
- Multiple failed login attempts
- An email administrator sees many bounced emails with suspicious content
- A network administrator notices an unusual deviation from typical network traffic flows

Technical Deep Dive: NIST Computer Security Incident Handling Guide

Questions to Consider

- Do devices that are used for our business, whether business-owned or employee-owned, have antivirus software installed?
- Do employees know how to detect possible cybersecurity attacks and how to report them?
- How is our business monitoring its logs and alerts to detect potential cyber incidents?

Related Resources

- Ransomware Protection and Response
- Detecting a Potential Intrusion
- Cybersecurity Training Resources

View all NIST CSF 2.0 Resources Here

RESPOND

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

Actions to Consider

Understand

- Understand what your incident response plan is and who has authority and responsibility for implementing various aspects of the plan. *(RS.MA-01)*

Assess

- Assess your ability to respond to a cybersecurity incident. *(RS.MA-01)*
- Assess the incident to determine its severity, what happened, and its root cause. *(RS.AN-03, RS.MA-03)*

Prioritize

- Prioritize taking steps to contain and eradicate the incident to prevent further damage. *(RS.MI)*

Communicate

- Communicate a confirmed cybersecurity incident with all internal and external stakeholders (e.g., customers, business partners, law enforcement agencies, regulatory bodies) as required by laws, regulations, contracts, or policies. *(RS.CO-02/03)*

Getting Started with an Incident Response Plan

Before an incident occurs, you want to be ready with a basic response plan. This will be customized based on the business but should include:

- ✓ **A business champion**: Someone who is responsible for developing and maintaining your incident response plan.
- ✓ **Who to call:** List all the individuals who may be part of your incident response efforts. Include their contact information, responsibilities, and authority.
- ✓ **What/when/how to report:** List your business's communications/reporting responsibilities as required by laws, regulations, contracts, or policies.

Technical Deep Dive: NIST Computer Security Incident Handling Guide

Contact	Phone
Business Leader:	
Technical Contact:	
State Police:	
Legal:	
Bank:	
Insurance:	

Questions to Consider

- Do we have a cybersecurity incident response plan? If so, have we practiced it to see if it is feasible?
- Do we know who the key internal and external stakeholders and decision-makers are who will assist if we have a confirmed cybersecurity incident?

Related Resources

- Incident Response Plan Basics
- FBI's Internet Crime Complaint Center
- Data Breach Response: A Guide for Business
- Best Practices for Victim Response and Reporting of Cyber Incidents

View all NIST CSF 2.0 Resources Here

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

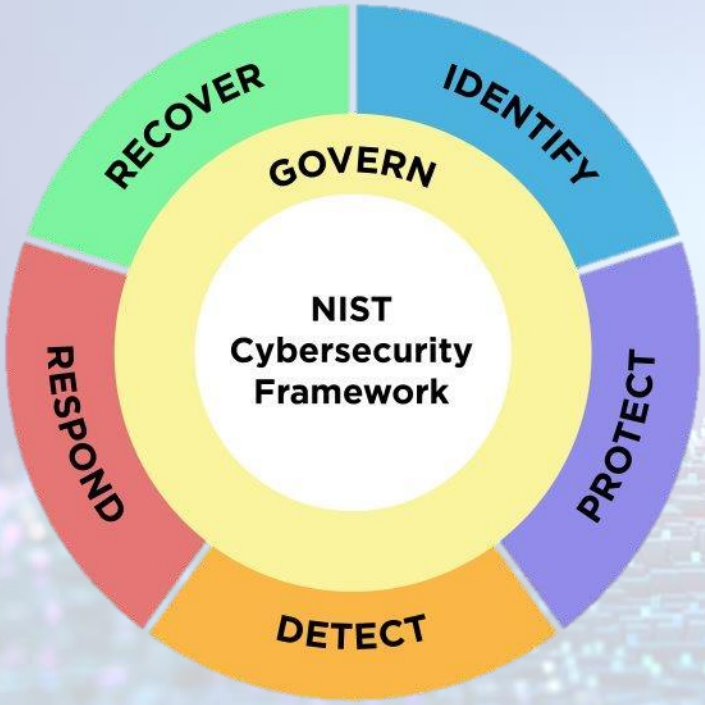
Questions to Consider

- 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



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

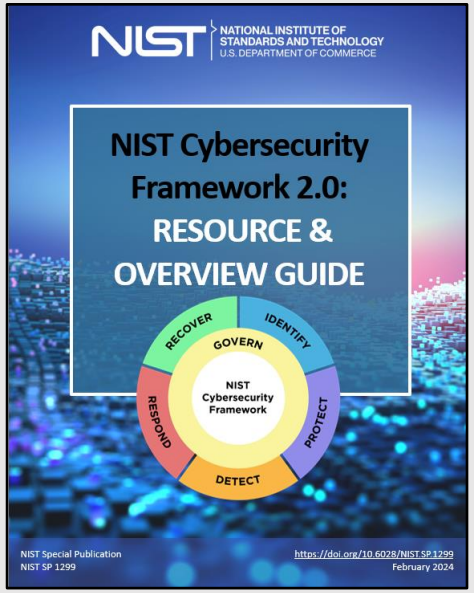
Additional CSF 2.0 Resources

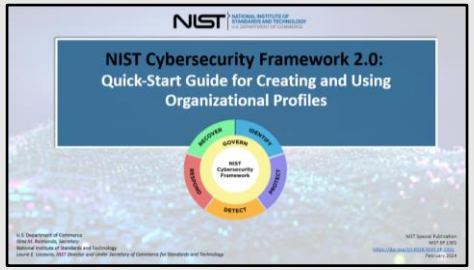
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

This webinar is being recorded

Explore All CSF 2.0 Resources

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





Navigating NIST's CSF 2.0 Quick Start Guides

Resource and Overview Guide

Understand the basics and learn about the many available helpful CSF 2.0 resources

Download

The below targeted guides will help you with specific topics.

CSF 2.0 Organizational Profiles
Guidance for organizations, with considerations for creating and using spreadsheets called *Profiles*, to implement the CSF 2.0.

Download

CSF 2.0 Community Profiles
This guide provides considerations for creating and using Community Profiles to implement the CSF 2.0 and support the needs of organizations in communities that share common priorities.

Download

Small Business
Resources specifically tailored to small businesses with modest or no cybersecurity plans currently in place.

Download

C-SCRM
Helps organizations become smarter acquirers and suppliers of technology products and services.

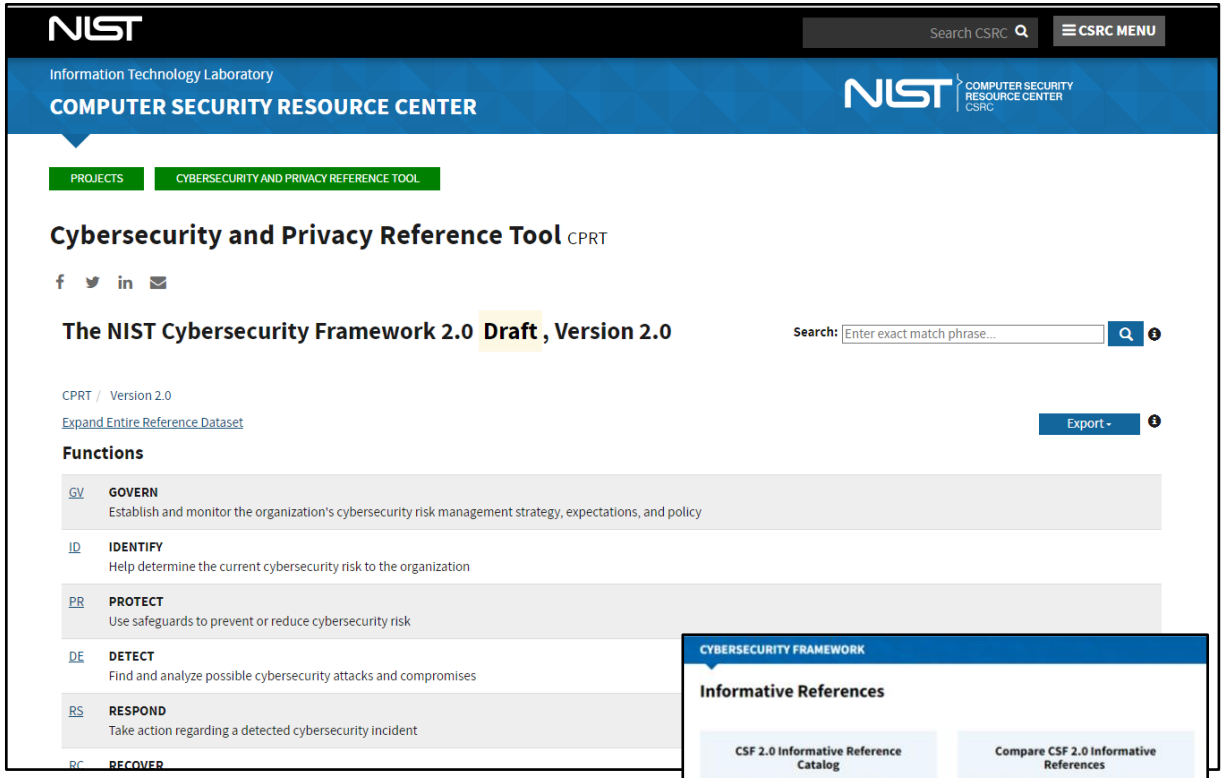
Download

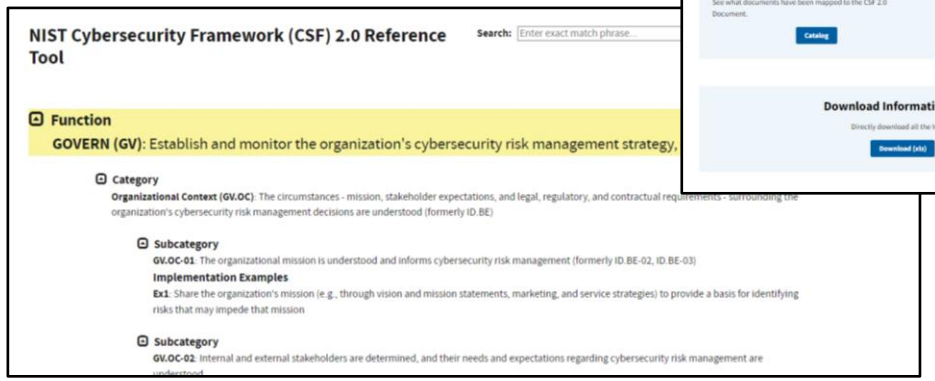
Tiers
Organizations can use these to apply the CSF 2.0 Tiers to Profiles to characterize the rigor of their cybersecurity risk governance and management outcomes.

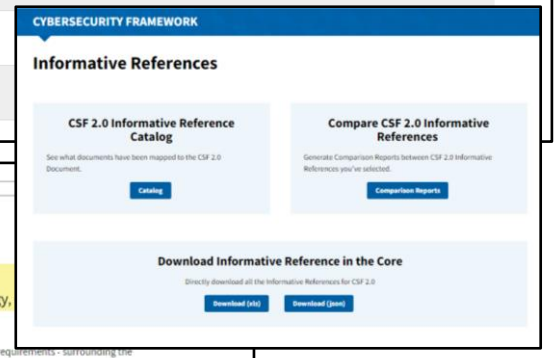
Download

Enterprise Risk Management
How ERM practitioners can utilize the outcomes provided in the CSF 2.0 to improve organizational cybersecurity risk management.

Download

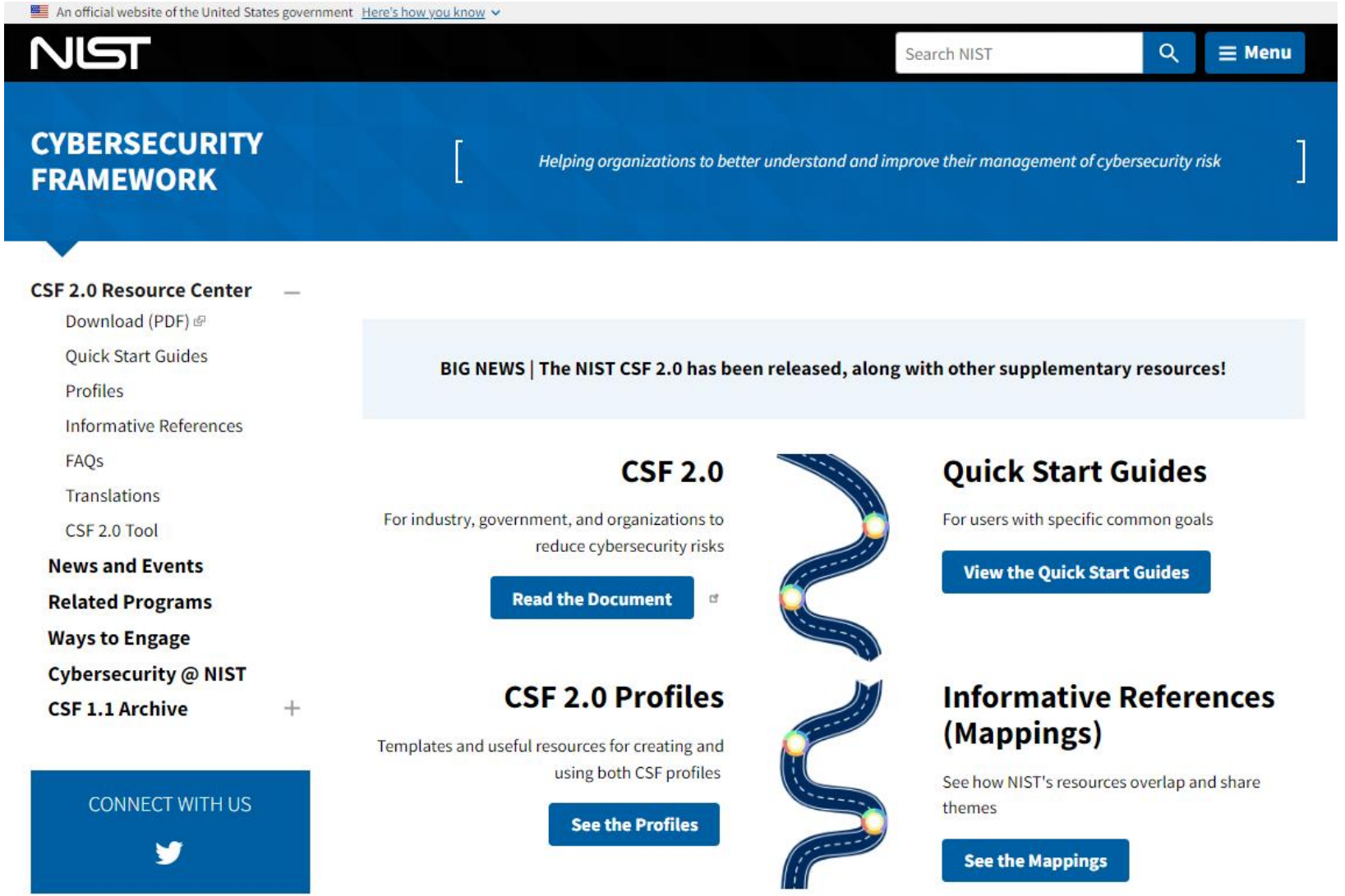






CSF 2.0 Resource Library

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



nist.gov/cyberframework

How to Get Involved/Upcoming Events

This webinar is being recorded

Join the Community of Interest

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

Convening companies, trade associations, and others who can share business insights, expertise, challenges, and perspectives to guide our work and assist NIST to better meet the cybersecurity needs of small businesses.

Over 9,500 individuals have already joined the full COI!

Subgroup	Meeting Dates	How to Join
SMB Owners/ Operators	~~February 14, 2024~~ **April 17, 2024** **July 17, 2024** **October 17, 2024**	Email: NIST-SMB-Owners+subscribe@list.nist.gov
SMB Vendors and Resource Partners	~~February 21, 2024~~ **April 24, 2024** **July 24, 2024** **October 24, 2024**	Email: NIST-SMB-Vendors+subscribe@list.nist.gov

Learn More Here: https://www.nist.gov/itl/smallbusinesscyber/get-engaged

Upcoming Webinar

Cybersecurity Resources for Small to Medium-Sized Manufacturers

A Fireside Chat with the NIST Manufacturing Extension Partnership (MEP)

May 2, 2024

2:00 PM -2:45 PM ET

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

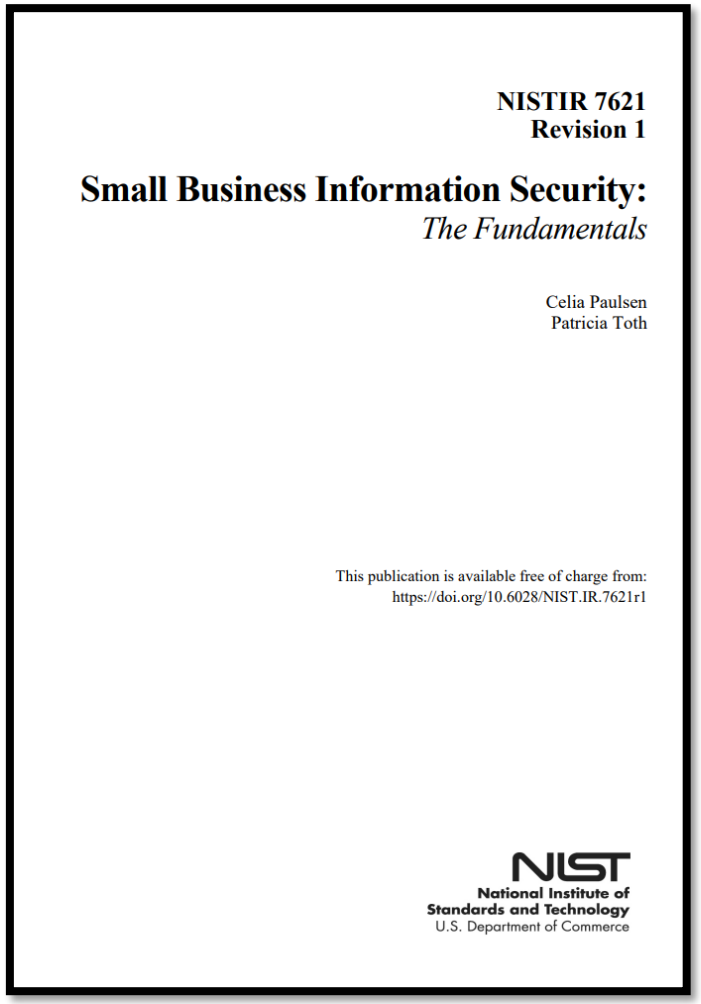
Register: https://www.nist.gov/itl/smallbusinesscyber/events

Small Business Information Security: The Fundamentals

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

Pre-draft call for comments now open.
Comments due by May 16, 2024.

- What specific topics in NIST IR 7621 are most useful to you?
- Is the document's current level of specificity appropriate, too detailed, or too general? If the level of specificity is not appropriate, how can it be improved?
- How can NIST improve the alignment between NIST IR 7621 and other frameworks and publications?
- What new cybersecurity capabilities, challenges, or topics should be addressed?
- What topics or sections currently in the document are out of scope, no longer relevant, or better addressed elsewhere?
- Are there other substantive suggestions that would improve the document?
- Are there additional appendices that would add value to the document?


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

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

https://csrc.nist.gov/pubs/ir/7621/r2/iprd

Q&A

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

Please use the WebEx Q&A window to enter your questions.

Quick Links:

- **CSF 2.0 Small Business Quick Start Guide:** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf
- **CSF 2.0 Website:** https://www.nist.gov/cyberframework
- **CSF 2.0 FAQs:** https://www.nist.gov/faqs
- **NIST International Cybersecurity and Privacy Resources:** https://www.nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources
- **NIST Small Business Cybersecurity Corner:** www.nist.gov/itl/smallbusinesscyber

This webinar is being recorded

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

Thank You for Joining Today's Webinar!

FOR FURTHER INFORMATION AND/OR QUESTIONS ABOUT OUR SMALL BUSINESS RESOURCES:

smallbizsecurity@nist.gov

FOR FURTHER INFORMATION AND/OR QUESTIONS ABOUT THE CYBERSECURITY FRAMEWORK:

cyberframework@nist.gov