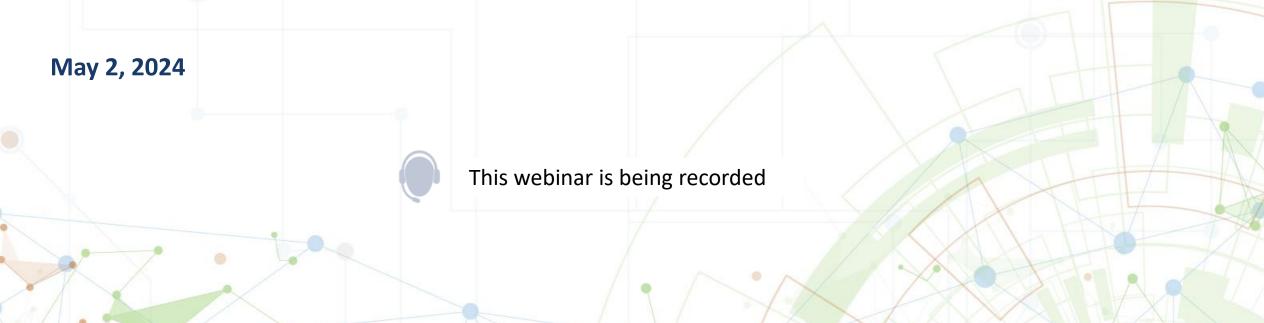
# **Cybersecurity Resources for Small to Medium-Sized Manufacturers:**

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







# Discussion



## **Panelists:**

- **Dr. Jyoti Malhotra**, Division Chief, National Programs, NIST MEP
- Savann Thorn, IT Specialist (Security), NIST MEP
- Daniel Eliot (moderator), Lead for Small Business Engagement, Applied Cybersecurity Division, NIST







### **Cybersecurity Resources for Manufacturers:**

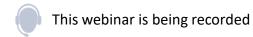
https://www.nist.gov/mep/cybersecurity-resources-manufacturers



### **Contact Your Local MEP Center:**

https://www.nist.gov/mep/contact-your-local-mep-center





# Finding NIST MFG-Related Publications



Information Technology Laboratory

### **COMPUTER SECURITY RESOURCE CENTER**



#### CURRENT PUBLICATIONS 4

#### NIST Series Pubs 1

Final Pubs

Drafts Open for Comment

Drafts (all)

View By Series 1

FIPS (standards)

SP 800 (guidance)

SP 1800 (practice guides)

SP (all subseries)

IR (interagency/internal reports)

CSWP (cybersecurity white papers)

ITL Bulletins

#### Other Pubs 1

**Project Descriptions** 

Journal Articles

Conference Papers

<u>Books</u>		
<u>Other</u>		
Search		
Manufactur	ing	
Search public	ation record data	
(not a full text	search)	
Sort By		
Release Dat	te (newest first) 🔻	-
Results Vie	ew	
Brief		~
Items Per I	Page 50 V	
Date		
//	<b>=====================================</b>	<b>=</b>
Status 🔁		
Final		
☐ Public [	Oraft	
□ Withdra	awn	

#### Search Results

Sorted By: × Release Date (newest first) Status: X Final Keywords: X Manufacturing

Showing 26 matching records.

Series	Number	Title	Status	Release Date
Project Description		Manufacturing Supply Chain Traceability with Blockchain Related Technology: Reference Implementation	Final	8/14/2023
CSWP	28	Security Segmentation in a Small Manufacturing Environment	Final	4/06/2023
Project Description		Responding to and Recovering from a Cyber Attack: Cybersecurity for the Manufacturing Sector (Rev. 1)	Final	12/22/2022
SP	800-161 Rev. 1	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations	Final	5/05/2022
IR	8419	Blockchain and Related Technologies to Support Manufacturing Supply Chain Traceability: Needs and Industry Perspectives	Final	4/07/2022
SP	1800-10	Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector	Final	3/16/2022
Journal Article		Cybersecurity Standards and Guidelines to Assist Small and Medium-Sized Manufacturers	Final	3/18/2021
IR	8183 Rev. 1	Cybersecurity Framework Version 1.1 Manufacturing Profile	Final	10/07/2020
IR	8219	Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection	Final	7/16/2020
IR	8259	Foundational Cybersecurity Activities for IoT Device Manufacturers	Final	5/29/2020
Project Description		Protecting Information and System Integrity in Industrial Control Systems Environments: Cybersecurity for the Manufacturing Sector	Final	2/07/2020

https://csrc.nist.gov/publications

NISTIR 8183 Revision 1

#### **Cybersecurity Framework Version 1.1 Manufacturing Profile**

Keith Stouffer Timothy Zimmerman



Aslam Sherule

https://doi.org/10



including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system devices such as

often found in the industrial sectors

and critical infrastructures. ICS control and monitor power generation and

and many varieties of manufacturing

distribution systems, hydroelectric

Many ICS began as proprietary,

and software. With no external

network connections, security focus

was primarily on physical threats to the equipment rather than network or cyber threats. Today, network

devices including Internet of Things

(IoT), Industrial IoT (IIoT), and other

information technology (IT) are being integrated into many ICS to

real-time business decisions. While this connectivity has delivered many benefits, it also increases the

allow operations data to support

vulnerability of these systems to

Industrial Control Systems (ICS) is

USNC CURRENT ®

Medium-Sized Manufacturers

standards were established with an other control system devices such as considered critical infrastructure, programmable logic controllers (PLCs) must maintain a higher level of data

Cybersecurity Standards and Guidelines to Assist Small an

dams, water treatment plants, oil and national security. For many ICS, it is unacceptable to degrade performance even for the sake of security. As a result, many organizations such as small and standards in ICS environments A concern of many SMMs is that

the operation of their manufacturing The National Institute of Standards and Technology (NIST) has recently released two publications to assist SMMs with developing and Framework Version 1.1 Manufacturing NISTIR 8183A (3 volumes), Profile and NISTIR 81834 (3

and system integrity, availability, and operational resilience for many reasons including economic Industrial Automation and Cont Systems and Organizations, and Control Objectives for Informatio and Related Technologies (COBI The Manufacturing Profile provi managing cybersecurity activit reducing cyber risk to manufact systems. It is meant to enhance standards and industry quideling CSF subcategory language releva-to the manufacturing domain with

outcomes and can be used to it

appartunities for improving the

manufacturing system

# Small Business Information Security: The Fundamentals





# 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

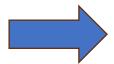
### **Small Business Information Security:**

The Fundamentals

Celia Paulsen Patricia Toth

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





# Upcoming In-Person Event

Cybersecurity Connections Event and Networking Lunch: Manufacturing and Operational Technology (OT) Cybersecurity

Date: Tuesday, May 21, 2024

Time: 11:00am–1:30pm

 Location: National Cybersecurity Center of Excellence (NCCoE), 9700 Great Seneca Hwy, Rockville, MD 20850

Registration for in-person attendance only:

https://www.nccoe.nist.gov/get-involved/attend-events





# **Panelists:**

- **Dr. Jyoti Malhotra**, Division Chief, National Programs, NIST MEP
- Savann Thorn, IT Specialist (Security), NIST MEP
- Daniel Eliot (moderator), Lead for Small Business Engagement, Applied Cybersecurity Division, NIST







### **Cybersecurity Resources for Manufacturers:**

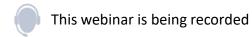
https://www.nist.gov/mep/cybersecurity-resources-manufacturers



### **Contact Your Local MEP Center:**

https://www.nist.gov/mep/contact-your-local-mep-center







# Thank You for Joining Today's Webinar!

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

smallbizsecurity@nist.gov

FOR FURTHER INFORMATION AND/OR QUESTIONS ABOUT THE NIST MEP NETWORK CYBERSECURITY RESOURCES:

mepcyber@nist.gov