NIST ICS Standards

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

nccoe.nist.gov

Agenda

- **NCCoE 101**
  - NCCoE overview
- **NIST CSF 2.0**
  - The NIST Cybersecurity Framework (CSF) 2.0
- **NIST 800 82 Rev 3**
  - Guide to Operational Technology (OT) Security
- **NISTIR 8183**
  - Cybersecurity Framework Version 1.1 Manufacturing Profile

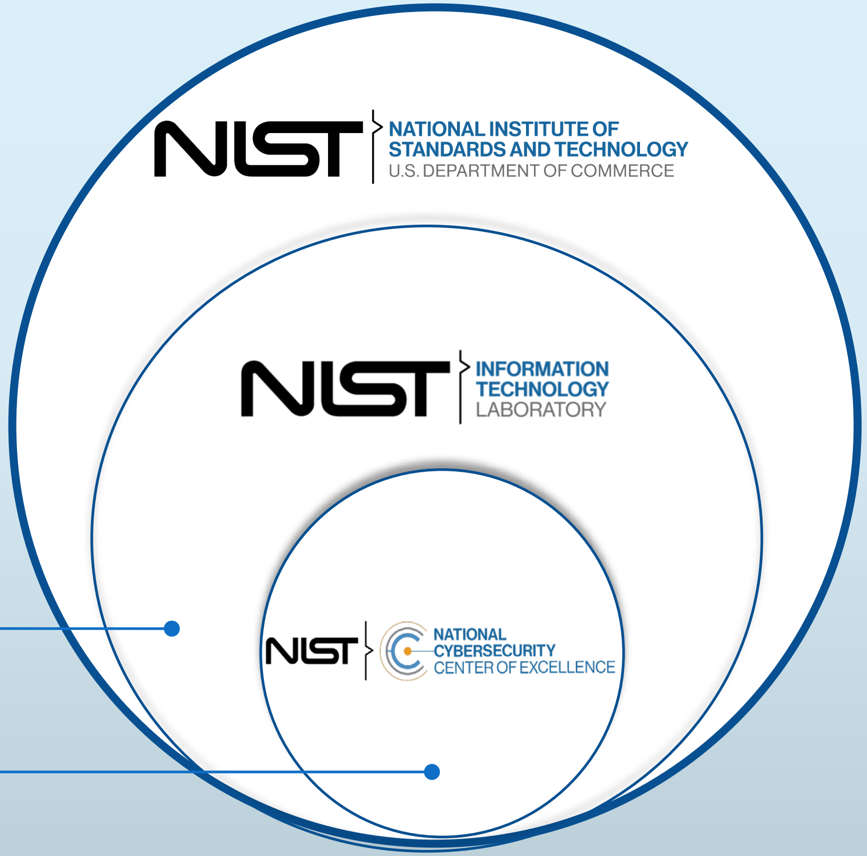
Who We Are

A solution-driven, collaborative hub addressing complex cybersecurity problems

Who We Are

Part of NIST, the NCCoE has access to a foundation of expertise, resources, relationships, and experience.

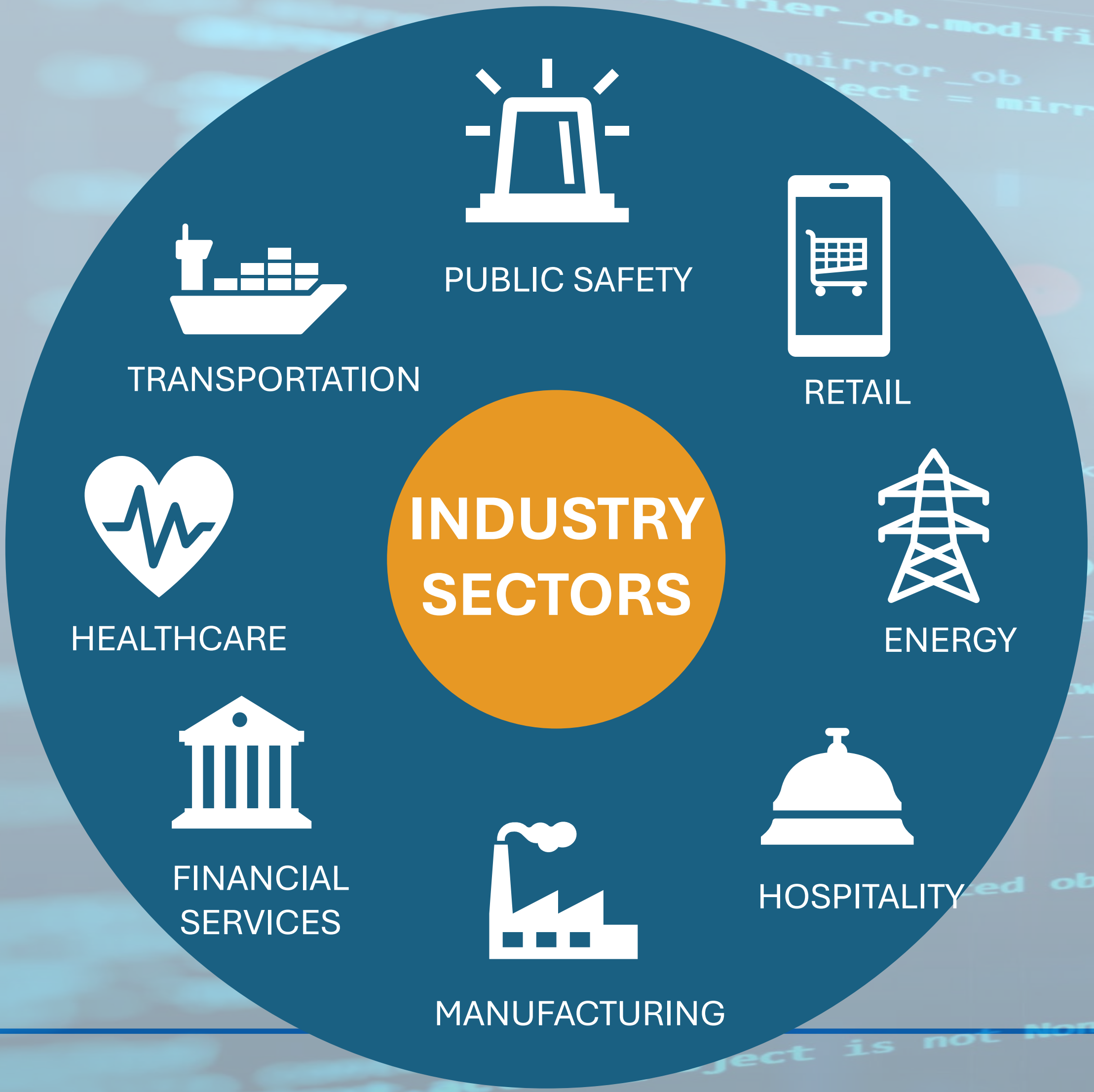
NIST is a **non-regulatory** agency. Our guidance is **voluntary**.


NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE
NIST INFORMATION TECHNOLOGY LABORATORY
NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Information Technology Laboratory

Applied Cybersecurity Division

Guidance Created With Industry, For Industry



INDUSTRY SECTORS

PUBLIC SAFETY

RETAIL

ENERGY

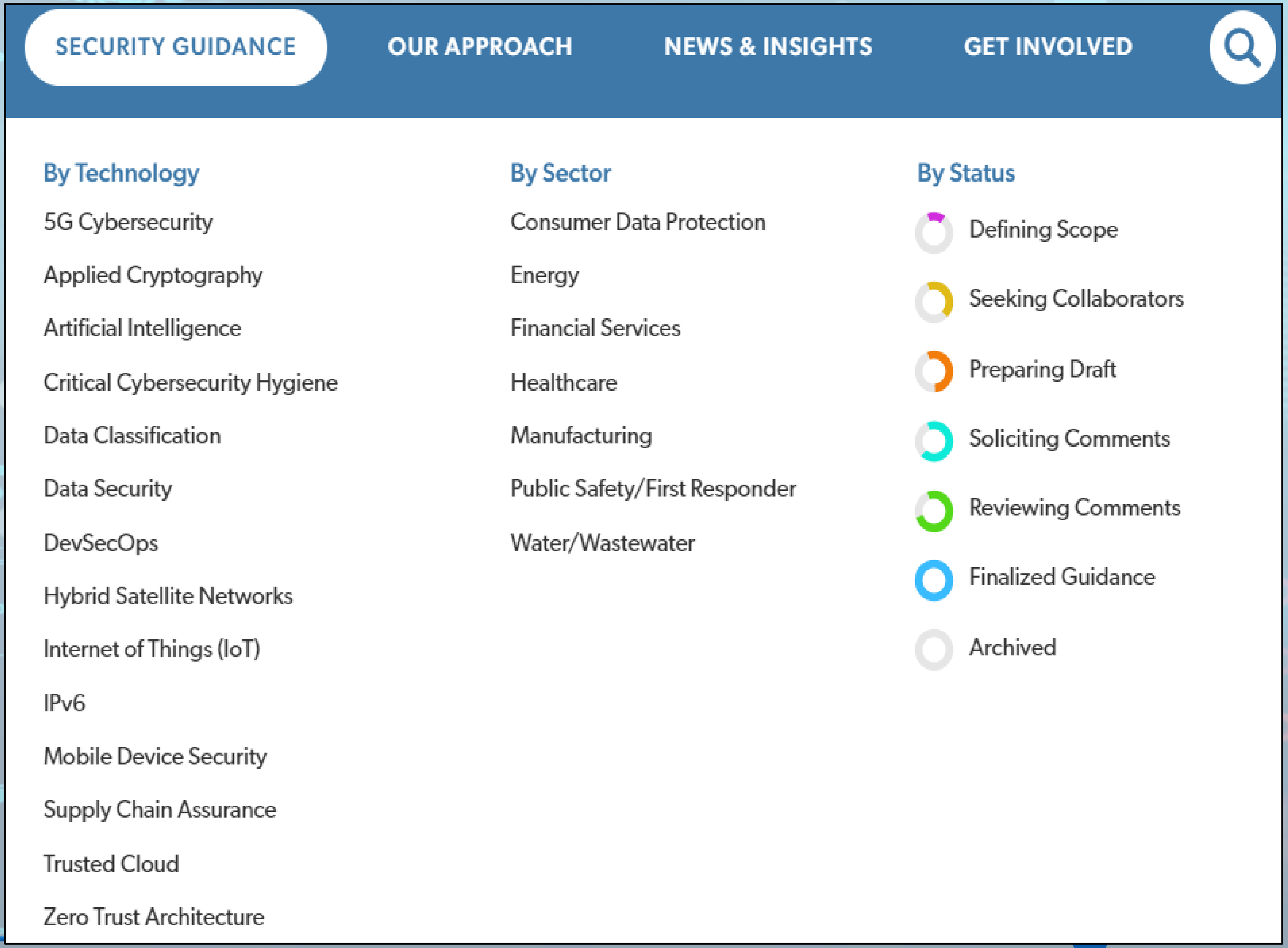
HOSPITALITY

MANUFACTURING

FINANCIAL SERVICES

HEALTHCARE

TRANSPORTATION



SECURITY GUIDANCE | OUR APPROACH | NEWS & INSIGHTS | GET INVOLVED

By Technology

- 5G Cybersecurity
- Applied Cryptography
- Artificial Intelligence
- Critical Cybersecurity Hygiene
- Data Classification
- Data Security
- DevSecOps
- Hybrid Satellite Networks
- Internet of Things (IoT)
- IPv6
- Mobile Device Security
- Supply Chain Assurance
- Trusted Cloud
- Zero Trust Architecture

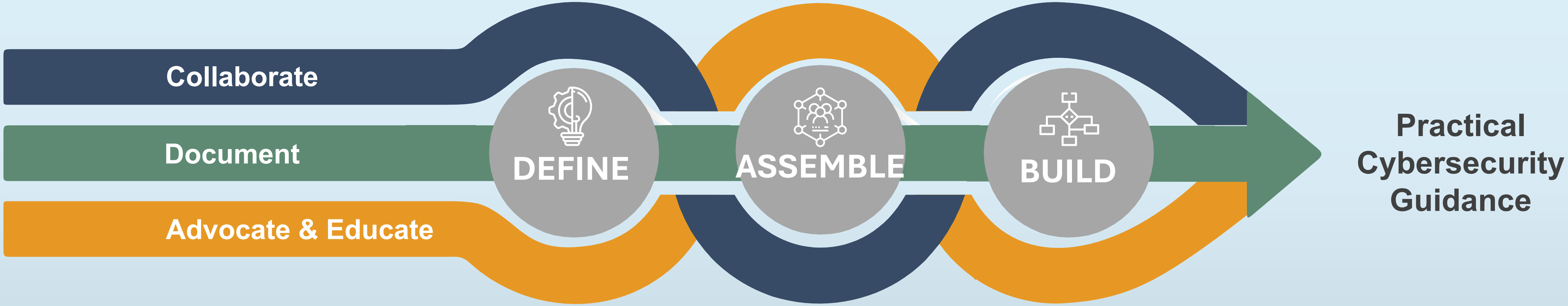
By Sector

- Consumer Data Protection
- Energy
- Financial Services
- Healthcare
- Manufacturing
- Public Safety/First Responder
- Water/Wastewater

By Status

- ○ Defining Scope
- ○ Seeking Collaborators
- ○ Preparing Draft
- ○ Soliciting Comments
- ○ Reviewing Comments
- ○ Finalized Guidance
- ○ Archived

Our Approach: A Foundation of Trust



Define a scope of work with industry to solve a pressing cybersecurity challenge

Assemble teams to address all aspects of the cybersecurity challenge

Build a practical, usable, repeatable demonstration to address the cybersecurity challenge

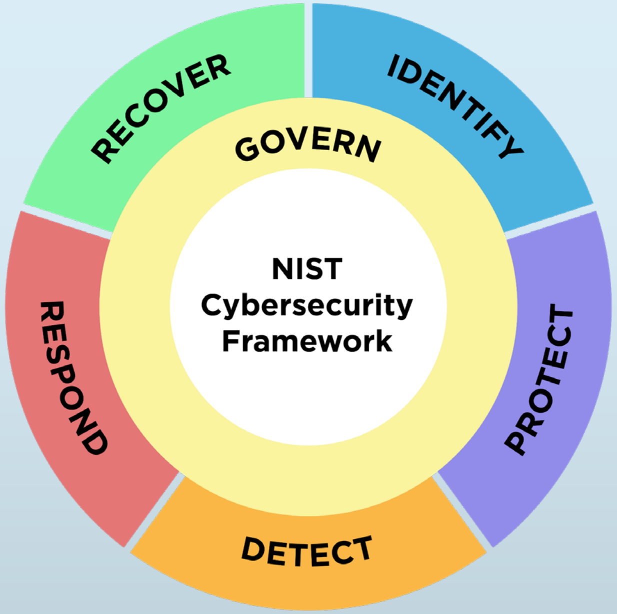
NIST's foundation of trust is based on an open, transparent, inclusive process.

NIST CSF 2.0

NIST Cybersecurity Framework (CSF)

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

- **What is it?**
  - Comprehensive list of cybersecurity outcomes to reduce cybersecurity risks to an organization – the "what", not "how" or "who"
  - Based on and mapped to international standards and resources
  - Adaptable to many technologies, sectors, maturity levels, and uses



NIST Cybersecurity Framework (CSF)

- **How is it used?**
  - **Understand and Assess:** Describe the current or target cybersecurity posture of part or all of an organization, determine gaps, and assess progress toward addressing those gaps.
  - **Prioritize:** Identify, organize, and prioritize actions for managing cybersecurity risks that align with the organization’s mission, legal and regulatory requirements, and risk management and governance expectations.
  - **Communicate:** Provide a common language for communicating inside and outside the organization about cybersecurity risks, capabilities, needs, and expectations.

CSF 2.0 Core

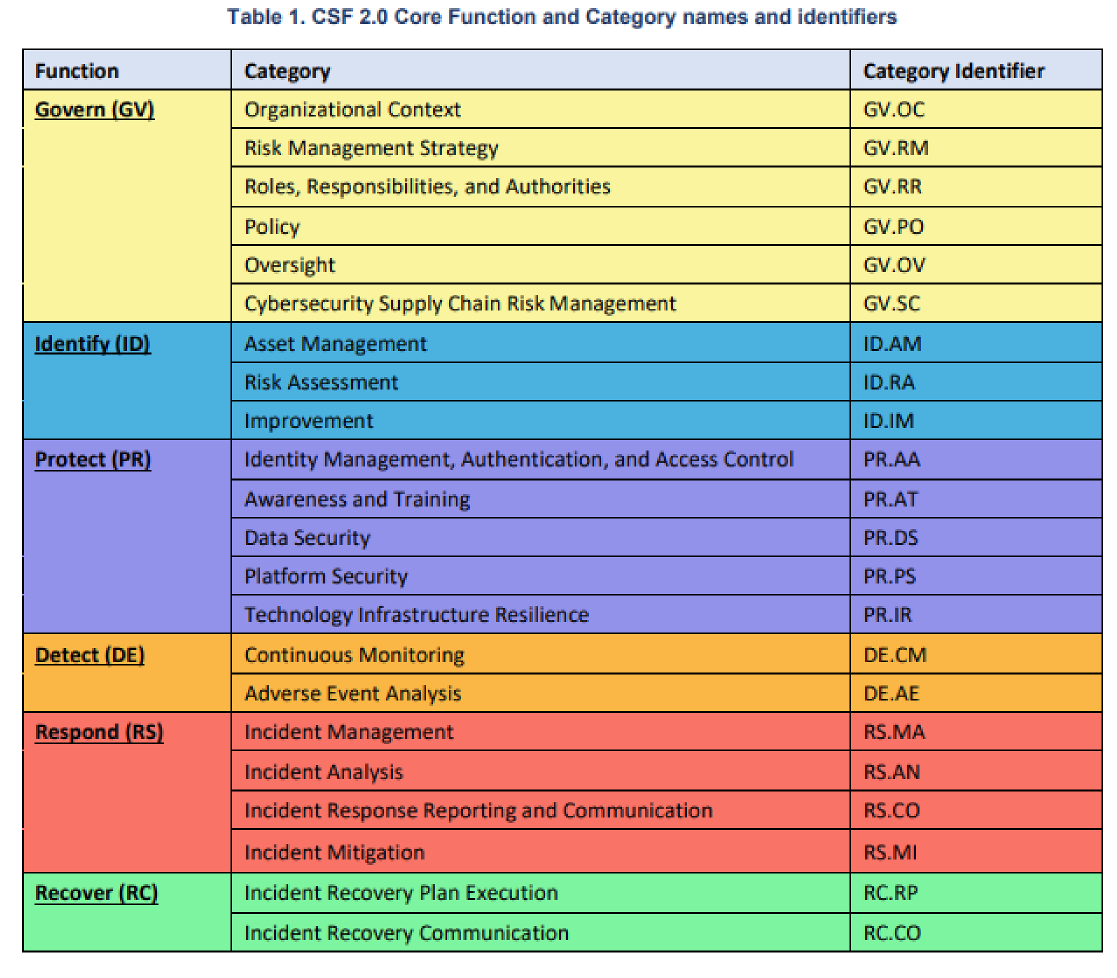


Table 1. CSF 2.0 Core Function and Category names and identifiers

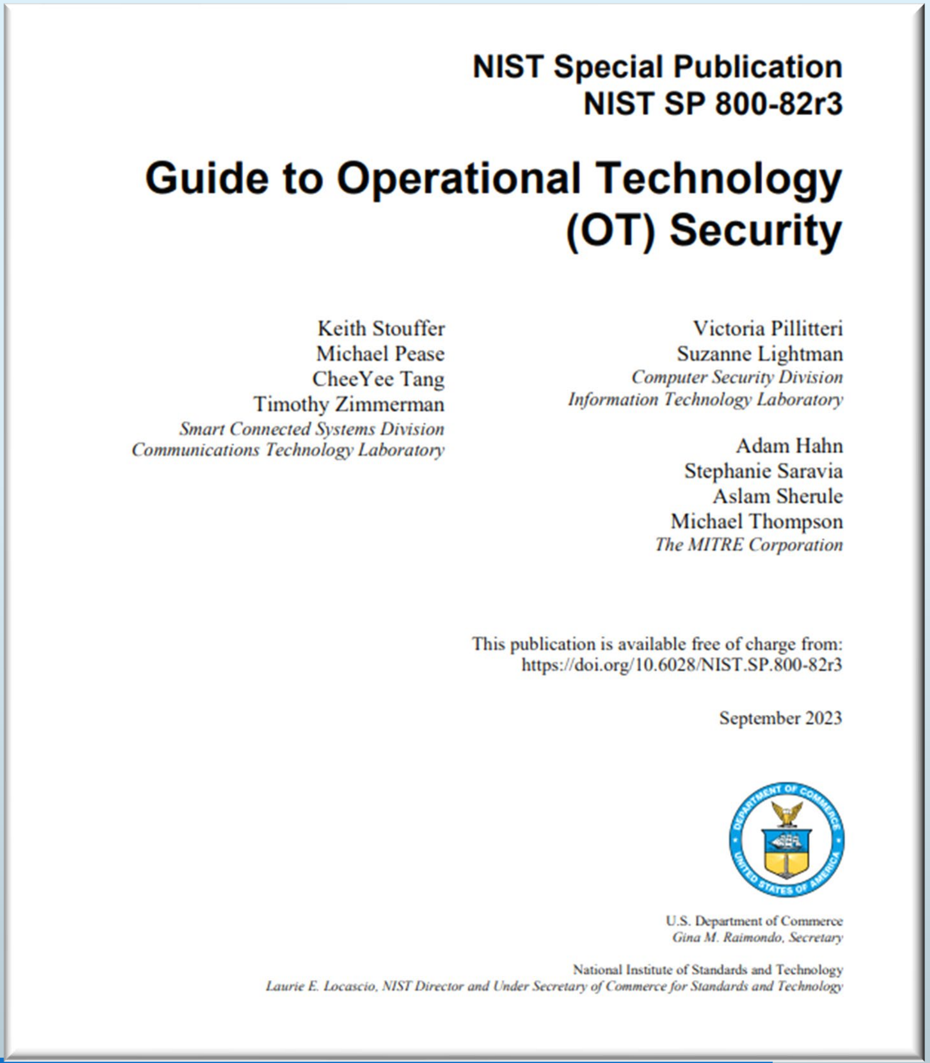
Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	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

RECOVER
IDENTIFY
FRAMEWORK
RESPOND
PROTECT
DETECT

NIST 800-82

SP 800-82 | History

- **Provides a comprehensive cybersecurity approach for securing ICS, while addressing unique performance, reliability, and safety requirements, including implementation guidance for NIST SP 800-53 controls**
- **Revisions**
  - Initial draft – September 2006
  - Revision 1 – May 2013
  - Revision 2 – May 2015
  - Revision 3 – September 2023
- **3,000,000+ downloads, 2400+ citations**



NIST Special Publication
NIST SP 800-82r3

Guide to Operational Technology (OT) Security

Keith Stouffer
Michael Pease
CheeYee Tang
Timothy Zimmerman
Smart Connected Systems Division
Communications Technology Laboratory

Victoria Pillitteri
Suzanne Lightman
Computer Security Division
Information Technology Laboratory

Adam Hahn
Stephanie Saravia
Aslam Sherule
Michael Thompson
The MITRE Corporation

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-82r3

September 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

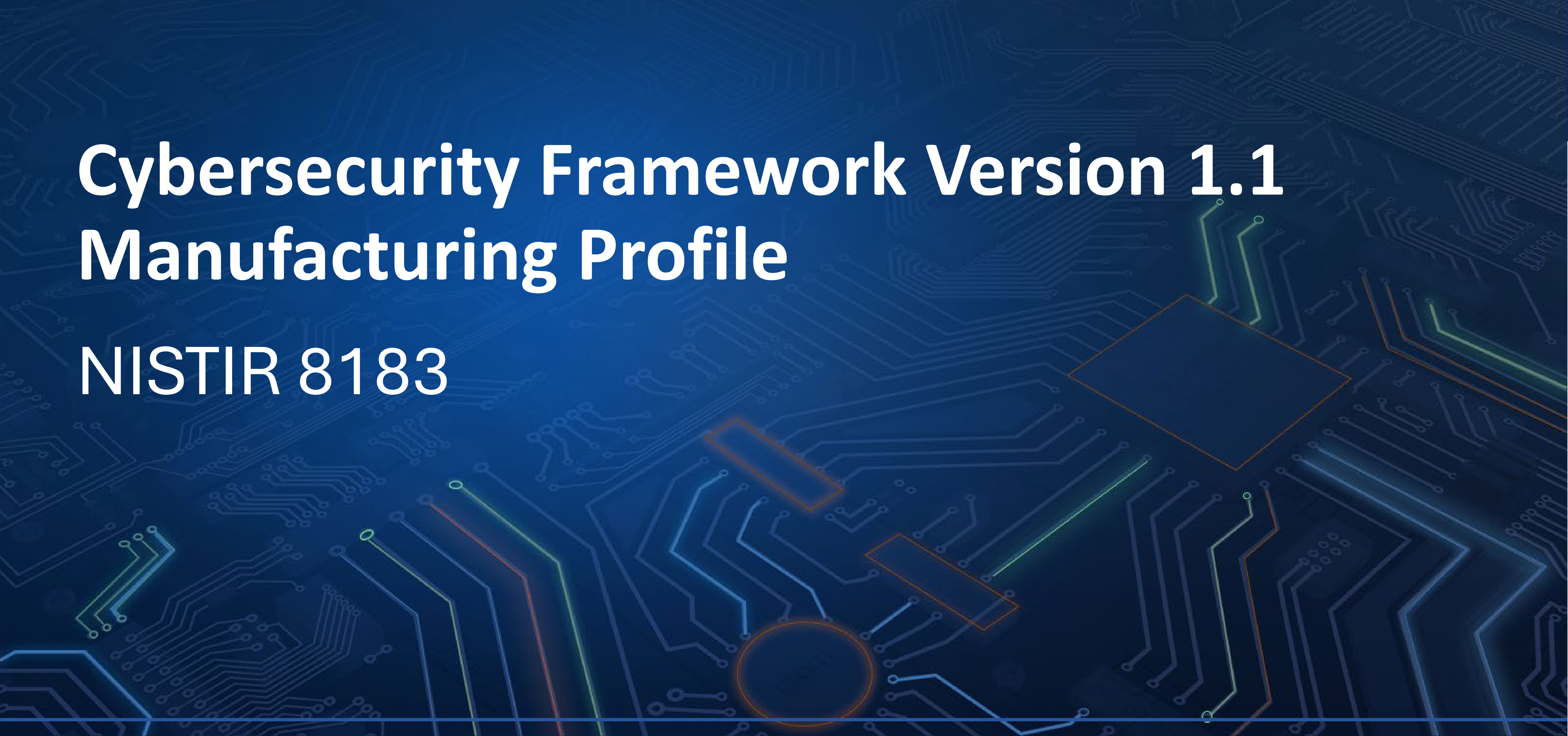
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

SP 800-82 | Revision 3

NIST updated SP 800-82 to incorporate lessons learned over the past several years, to provide alignment to relevant NIST guidance, to provide alignment to other relevant control system cybersecurity standards and recommended practices, and to address changes in the threat landscape. SP 800-82, Revision 3, Guide to Operational Technology (OT) Security was published September 2023.

Updates include:

- Expansion in scope from ICS to control systems/OT in general
- Application of new cybersecurity capabilities in control system/OT environments
- Updates to control system/OT threats, vulnerabilities, standards, and recommended practices
- Additional alignment with other OT security standards and guidelines, including the Cybersecurity Framework (CSF)
- New tailoring guidance for NIST SP 800-53, Rev. 5 security controls
- An OT overlay for NIST SP 800-53, Rev. 5 security controls that provides tailored security control baselines for low-impact, moderate-impact, and high-impact OT systems.



Cybersecurity Framework Version 1.1 Manufacturing Profile

NISTIR 8183

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

nccoe.nist.gov

NISTIR 8183 Rev.1 CSF Manufacturing Profile

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

- Provides the CSF Version 1.1 implementation details developed for the manufacturing environment
- Can be used as a roadmap for reducing cybersecurity risk for manufacturers that is aligned with manufacturing sector goals and industry best practices
- Provides a voluntary, risk-based approach for managing cybersecurity activities and reducing cyber risk to manufacturing systems
- Meant to enhance but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing

Manufacturing Profile Implementation Guidance

- Many small and medium-sized manufacturers have expressed challenges in implementing a cybersecurity program.
- Goal – Develop an Implementation Guide that drives the CSF Manufacturing Profile to practice and enables manufacturers to select and deploy cybersecurity tools and techniques that best fit their needs while addressing the demanding system operational performance, reliability, and safety requirements.
- Implement CSF Manufacturing Profile in the Cybersecurity for Smart Manufacturing Testbed
- Measure manufacturing system network, device and operational performance impacts when instrumented with cybersecurity protections in accordance with the Manufacturing Profile
- Develop guidance on how to implement the CSF in manufacturing environments while minimizing negative performance impacts

Use Case Implementation Results

- **The results of the two proof-of-concept implementations (Volume 2 and Volume 3) include:**
  - 44 cybersecurity tool and technique implementations
  - Over 80 network, device and operational performance impact measurements per implementation that had a potential to impact the manufacturing system
  - Over 125 GBs of measurement data available to the public
  - 12 example cybersecurity policy and procedure documents

Manufacturing Profile Implementation Guide

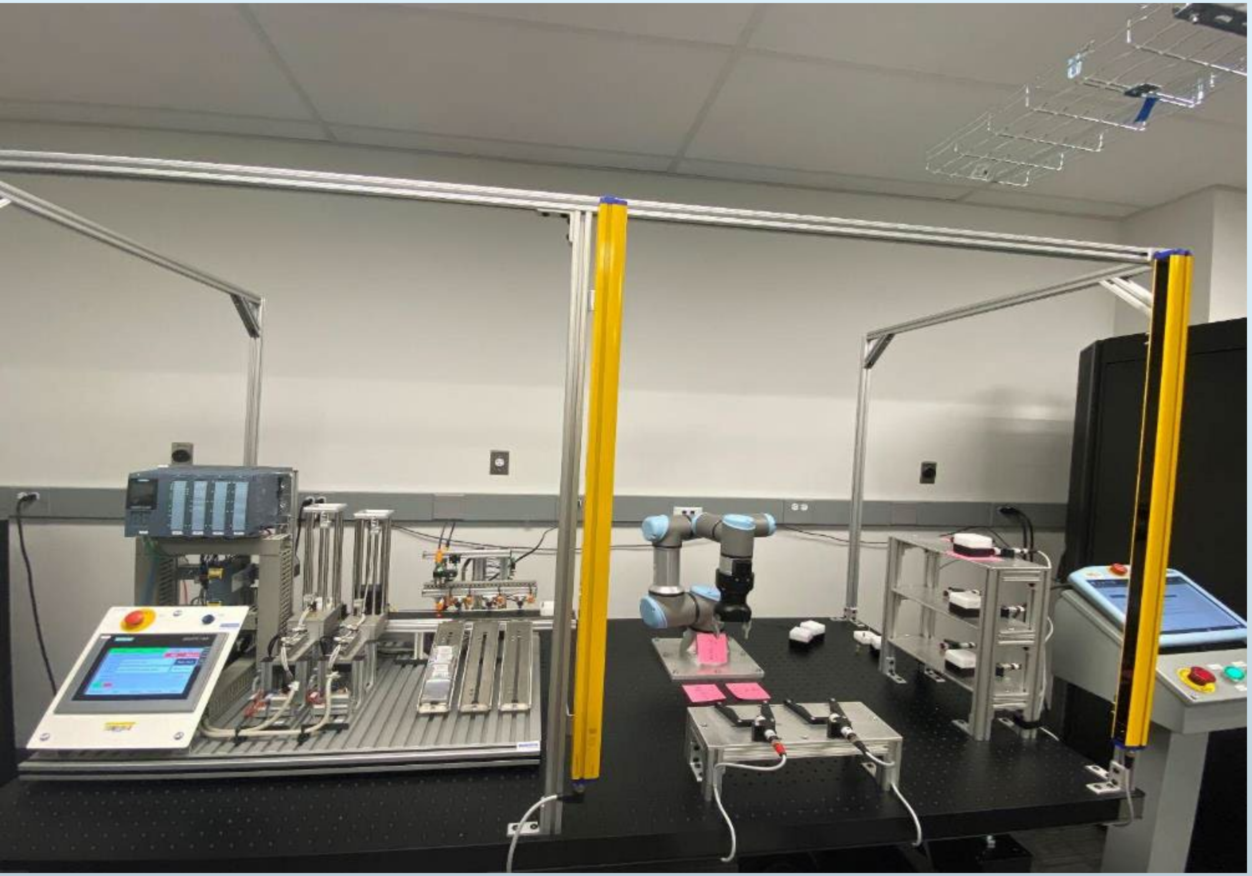
- **NISTIR 8183A Volume 1, Cybersecurity Framework Manufacturing Profile**
- **Low Security Level Example Implementations Guide**

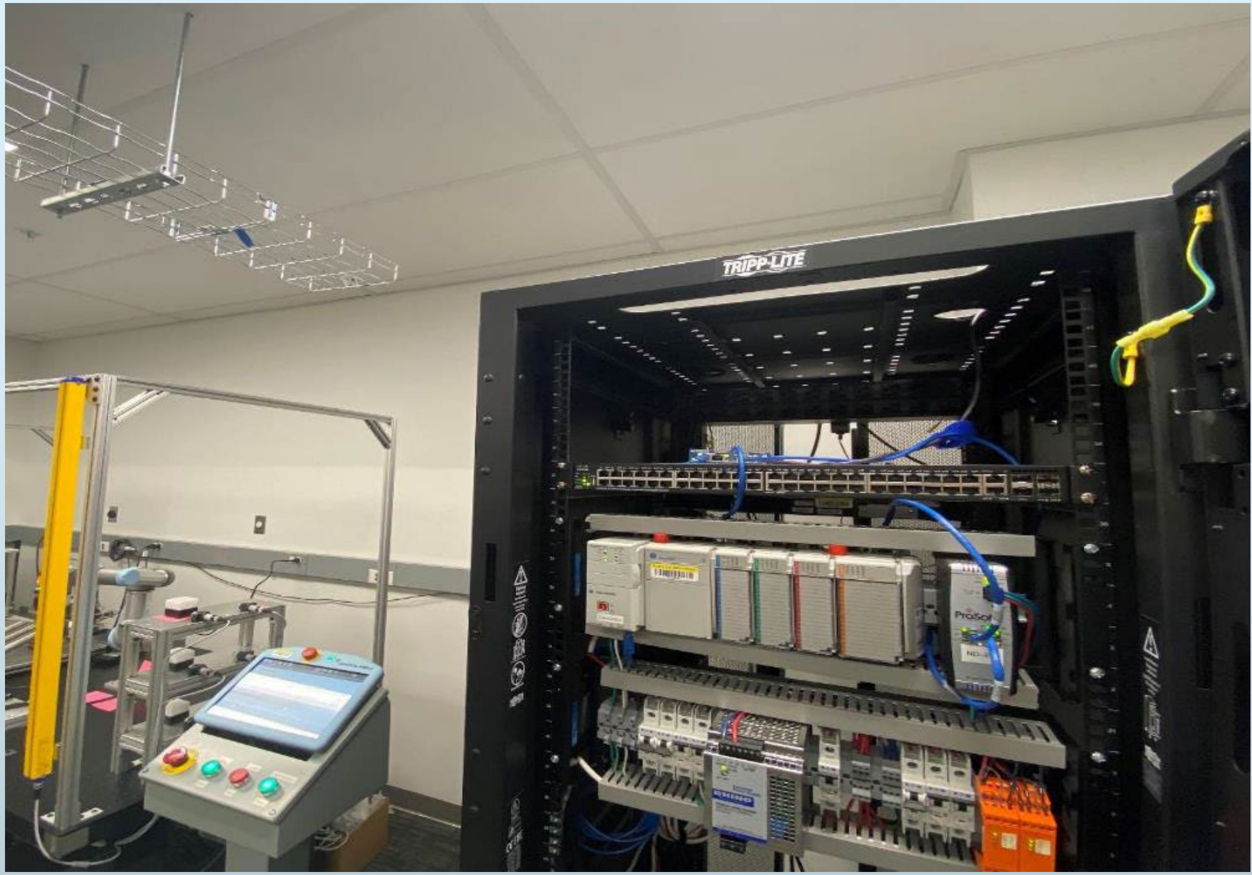
Volume 1
General Implementation Guidance

Volume 2
Process-based Manufacturing System Use Case

Volume 3
Discrete-based Manufacturing System Use Case

NCCoE Manufacturing Testbed





National Cybersecurity Center of Excellence (NCCoE)

Behavioral Anomaly Detection Project

https://www.nccoe.nist.gov/projects/use-cases/manufacturing/capabilities-assessment-securing-manufacturing-industrial-control-systems

System and Data Integrity Project

https://www.nccoe.nist.gov/projects/use-cases/manufacturing/integrity-ics

Respond and Recovery Project

https://www.nccoe.nist.gov/manufacturing/responding-and-recovering-cyber-attack

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Dr. Michael Powell

Principal Investigator
NIST/NCCoE
michael.powell@nist.gov

NCCoE Manufacturing Community of Interest
manufacturing_nccoe@nist.gov

nccoe.nist.gov

@NISTcyber