The NIST Cybersecurity Framework

U.S. German Standards Panel 2018

April 10, 2018

Adam.Sedgewick@nist.gov

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

National Institute of Standards and Technology

About NIST

- Agency of U.S. Department of Commerce
- NIST's mission is to develop and promote measurement, standards and technology to enhance productivity, facilitate trade, and improve the quality of life.
- Federal, non-regulatory agency around since 1901

NIST Cybersecurity

- Cybersecurity since the 1970s
- Computer Security Resource Center – csrc.nist.gov

NIST Priority Research Areas


Advanced Manufacturing


IT and Cybersecurity


Healthcare

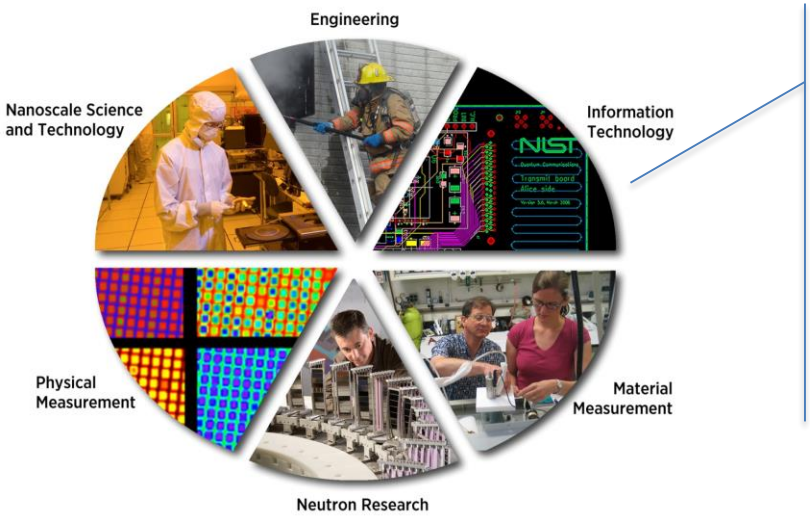

Forensic Science


Disaster Resilience


Cyber-physical Systems


Advanced Communications

NIST's Cybersecurity Portfolio



Cultivate trust in U.S. information and systems through research, development, and application of cybersecurity and privacy standards, guidelines, tools, and reference resources.

Biometrics – Software Assurance – Domain Name Security – Identity Management – FISMA – Security Automation – National Vulnerability Database – Configuration Checklists – Digital Signatures – Risk Management – Authentication – IPv6 Security Profile – Supply Chain – NICE – Health IT Security – Key Management – Secure Hash – PKI – Privacy Engineering– Smart Grid – Continuous Monitoring – Small Business Outreach – Mobile Devices – Standards – Cloud Computing – Usability – NSTIC – Passwords – Hardware Security – Electronic Voting – Wireless – Security Awareness – Vulnerability Measurement – Security Metrics – Public Safety Communications – NCCoE

Cybersecurity Framework *Current* Charter

Improving Critical Infrastructure Cybersecurity

February 12, 2013

"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"

Executive Order 13636

December 18, 2014

Amends the National Institute of Standards and Technology Act (15 U.S.C. 272(c)) to say:

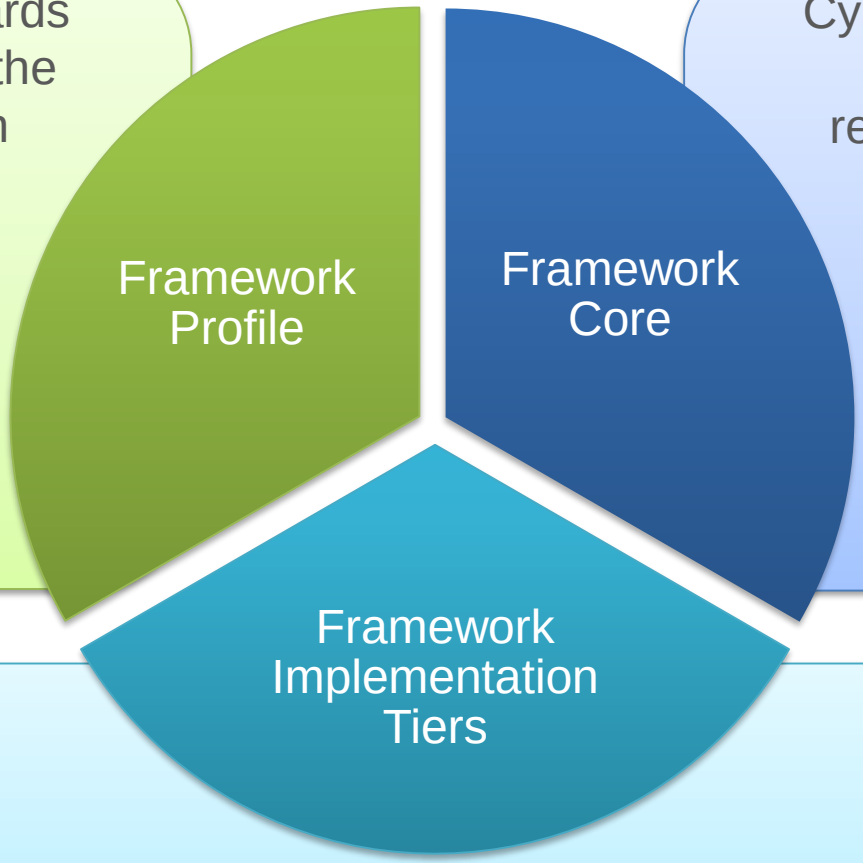
"…on an ongoing basis, facilitate and support the development of a ***voluntary***, ***consensus-based***, ***industry-led*** *set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure"*

Cybersecurity Enhancement Act of 2014 (P.L. 113-274)

Cybersecurity Framework Components

Aligns industry standards and best practices to the Framework Core in an implementation scenario

Supports prioritization and measurement while factoring in business needs



Cybersecurity activities and informative references, organized around particular outcomes

Enables communication of cyber risk across an organization

Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

Core

A Catalog of Cybersecurity Outcomes

	Function	Category
What processes and assets need protection?	**Identify**	Asset Management
		Business Environment
		Governance
		Risk Assessment
		Risk Management Strategy
What safeguards are available?	**Protect**	Access Control
		Awareness and Training
		Data Security
		Information Protection Processes & Procedures
		Maintenance
		Protective Technology
What techniques can identify incidents?	**Detect**	Anomalies and Events
		Security Continuous Monitoring
		Detection Processes
What techniques can contain impacts of incidents?	**Respond**	Response Planning
		Communications
		Analysis
		Mitigation
		Improvements
What techniques can restore capabilities?	**Recover**	Recovery Planning
		Improvements
		Communications

Core – Example

Cybersecurity Framework Component

Function	Category	Subcategory	Informative Reference
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	• **CCS CSC** 16 • **COBIT 5** DSS05.04, DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.5.1 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 • **NIST SP 800-53 Rev. 4** AC-2, IA Family
		PR.AC-2: Physical access to assets is managed and protected	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 • **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
		PR.AC-3: Remote access is managed	• **COBIT 5** APO13.01, DSS01.04, DSS05.03 • **ISA 62443-2-1:2009** 4.3.3.6.6 • **ISA 62443-3-3:2013** SR 1.13, SR 2.6 • **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1

Profile

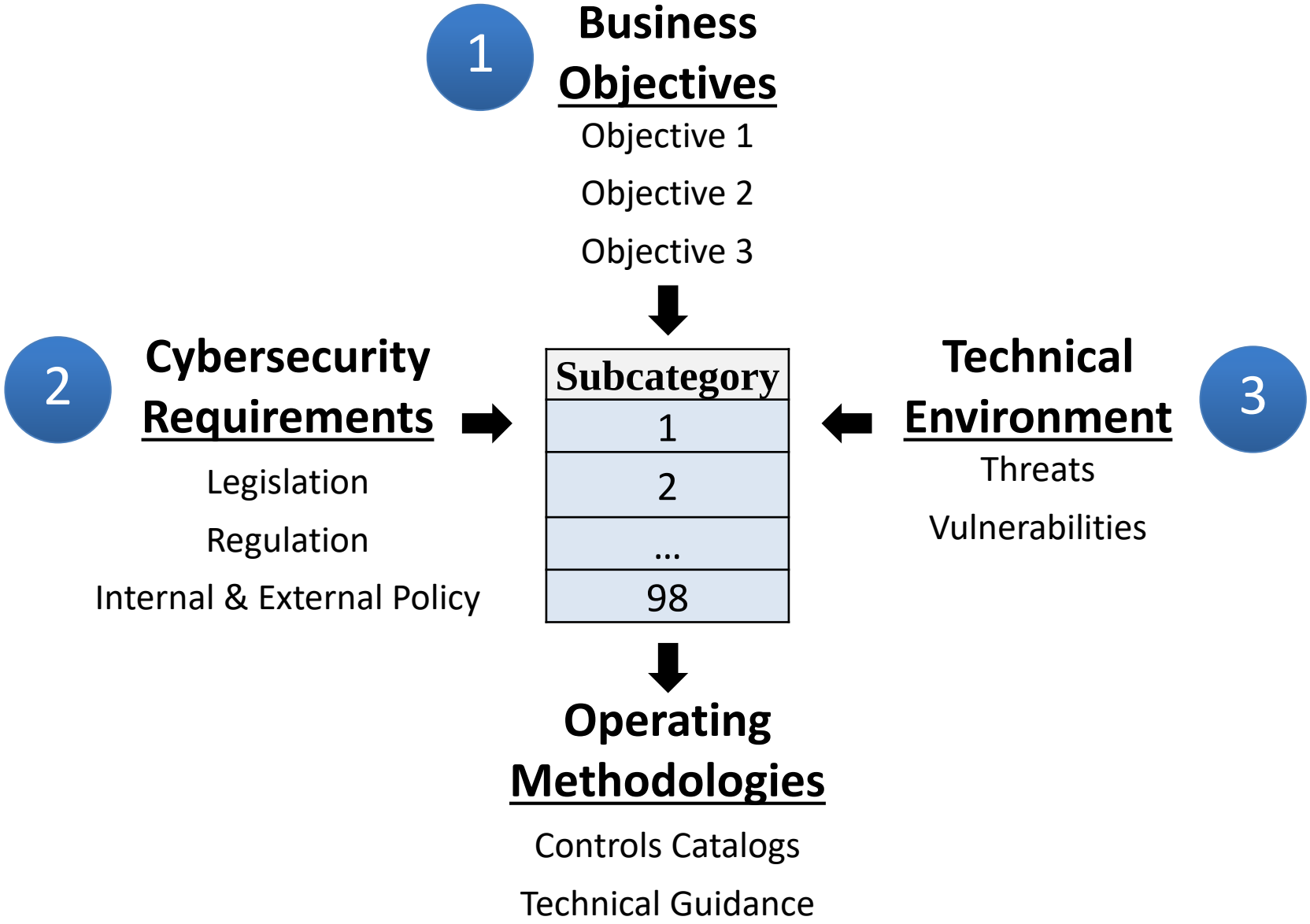
Customizing Cybersecurity Framework

Ways to think about a Profile:

- A customization of the Core for a given sector, subsector, or organization
- A fusion of business/mission logic and cybersecurity outcomes
- An alignment of cybersecurity requirements with operational methodologies
- A basis for assessment and expressing target state
- A decision support tool for cybersecurity risk management

Profile Foundational Information

A Profile Can be Created from Three Types of Information



Key Framework Attributes

Principles of the Current and Future Versions of Framework

Common and accessible language

- Understandable by many professionals

It's adaptable to many sectors and uses

- Meant to be *customized*

It's risk-based

- A Catalog of cybersecurity outcomes
- Does provide *how* or *how much* cybersecurity is appropriate

It's meant to be paired

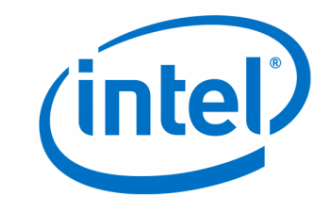
- Take advantage of great pre-existing things

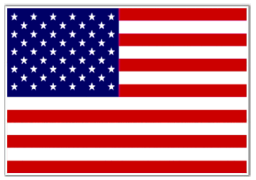
It's a living document

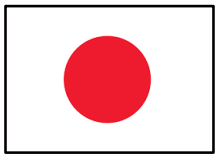
- Enable best practices to become *standard practices for everyone*
- Can be updated as *technology and threats* change
- Evolves *faster* than regulation and legislation
- Can be updated as stakeholders *learn from implementation*

Cybersecurity Framework Use

Framework for Improving Critical Infrastructure Cybersecurity







AT&T

NTT
NIPPON TELEGRAPH AND TELEPHONE CORPORATION

THE UNIVERSITY OF CHICAGO

Examples of Framework Industry Resources

www.nist.gov/cyberframework/industry-resources

Italy's National Framework for Cybersecurity

American Water Works Association's *Process Control System Security Guidance for the Water Sector*

The Cybersecurity Framework in Action: An Intel Use Case

Cybersecurity Risk Management and Best Practices Working Group 4: Final Report

Financial Services Sector Specific Cybersecurity "Profile"

Recent NIST Work Products

www.nist.gov/cyberframework/industry-resources

Manufacturing Profile

NIST Discrete Manufacturing Cybersecurity Framework Profile

Self-Assessment Criteria

Baldrige Cybersecurity Excellence Builder

Maritime Profile

U.S. Coast Guard Bulk Liquid Transport Profile

Proposed U.S. Federal Usage

NIST IR 8170 The Cybersecurity Framework: Implementation Guidance for Federal Agencies

Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
Executive Order 13800

1. **Integrate enterprise and cybersecurity risk management**
2. **Manage cybersecurity requirements**
3. **Integrate and align cybersecurity and acquisition processes**
4. **Evaluate organizational cybersecurity**
5. **Manage the cybersecurity program**
6. **Maintain a comprehensive understanding of cybersecurity risk** *(supports RMF Authorize)*
7. **Report cybersecurity risks** *(supports RMF Monitor)*
8. **Inform the tailoring process** *(supports RMF Select)*

Major Themes from Inputs: Draft #2

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

Additional major themes addressed by Draft #2:

- Provides guidance for self-assessment, including use of Framework-based measurement
- Enhances guidance applying the Framework to manage cybersecurity within supply chains and for acquisition decisions
- Better accounts for Authorization, Authentication, and Identity Proofing
- Accounts for emerging vulnerability information (a.k.a., Coordinated Vulnerability Disclosure)
- Refinement of Implementation Tier criteria
- Clarity on Implementation Tiers and their relationship to Profiles

Resources

Where to Learn More and Stay Current

Framework for Improving Critical Infrastructure Cybersecurity and related news and information:
www.nist.gov/cyberframework

Additional cybersecurity resources:
http://csrc.nist.gov/

Questions, comments, ideas:
cyberframework@nist.gov