The Framework for Improving Critical Infrastructure Cybersecurity

Matthew Barrett

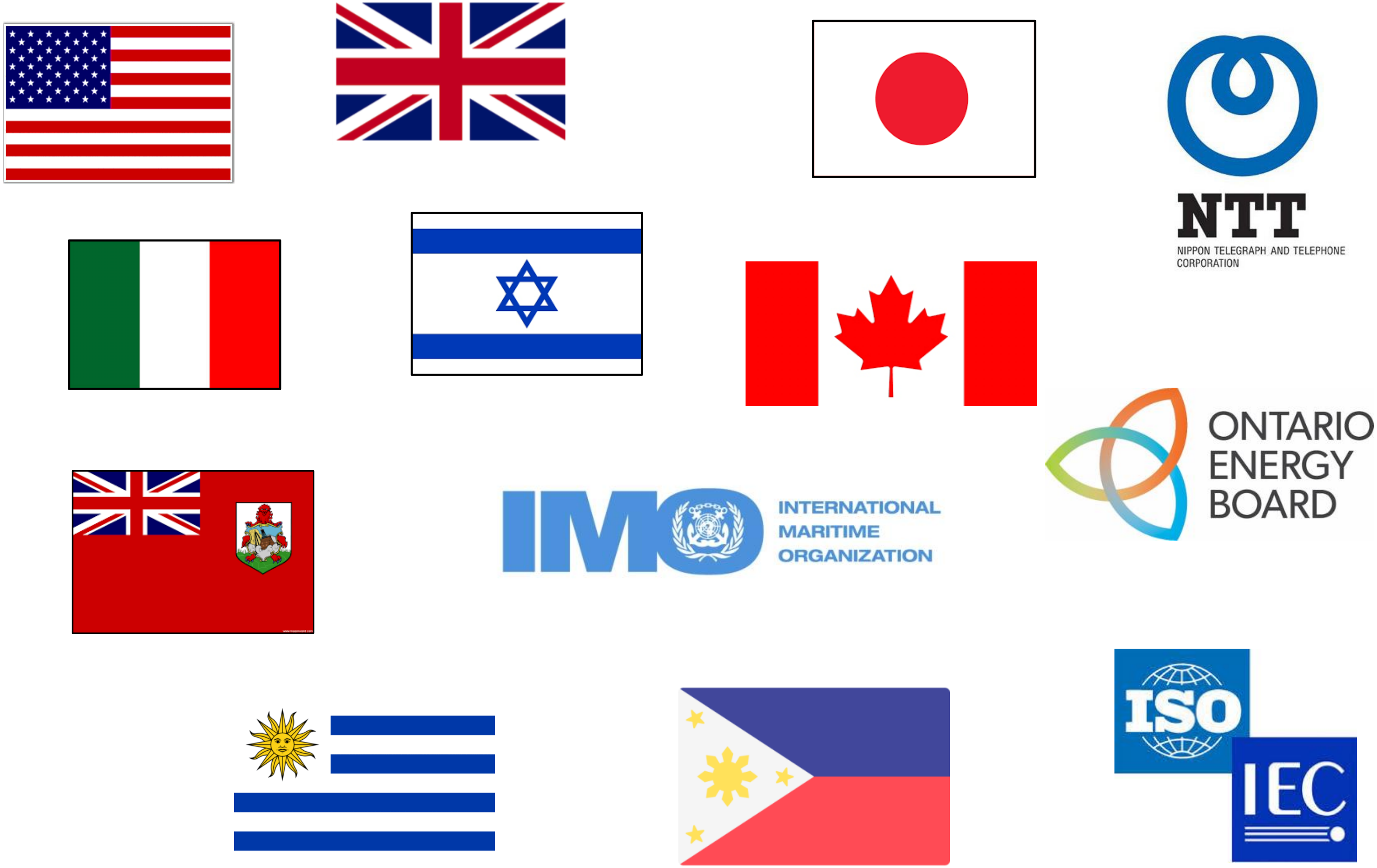
September 2018

cyberframework@nist.gov

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

International Use

Framework for Improving Critical Infrastructure Cybersecurity


NTT
NIPPON TELEGRAPH AND TELEPHONE CORPORATION
ONTARIO ENERGY BOARD
IMO
INTERNATIONAL MARITIME ORGANIZATION
ISO
IEC

Core

A Catalog of Cybersecurity Outcomes

	Function
Understand risks	**Identify**
Determine safeguards	**Protect**
Identify events	**Detect**
Address incidents	**Respond**
Restore capabilities	**Recover**

- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction

Core

A Catalog of Cybersecurity Outcomes

What processes and assets need protection?

What safeguards are available?

What techniques can identify incidents?

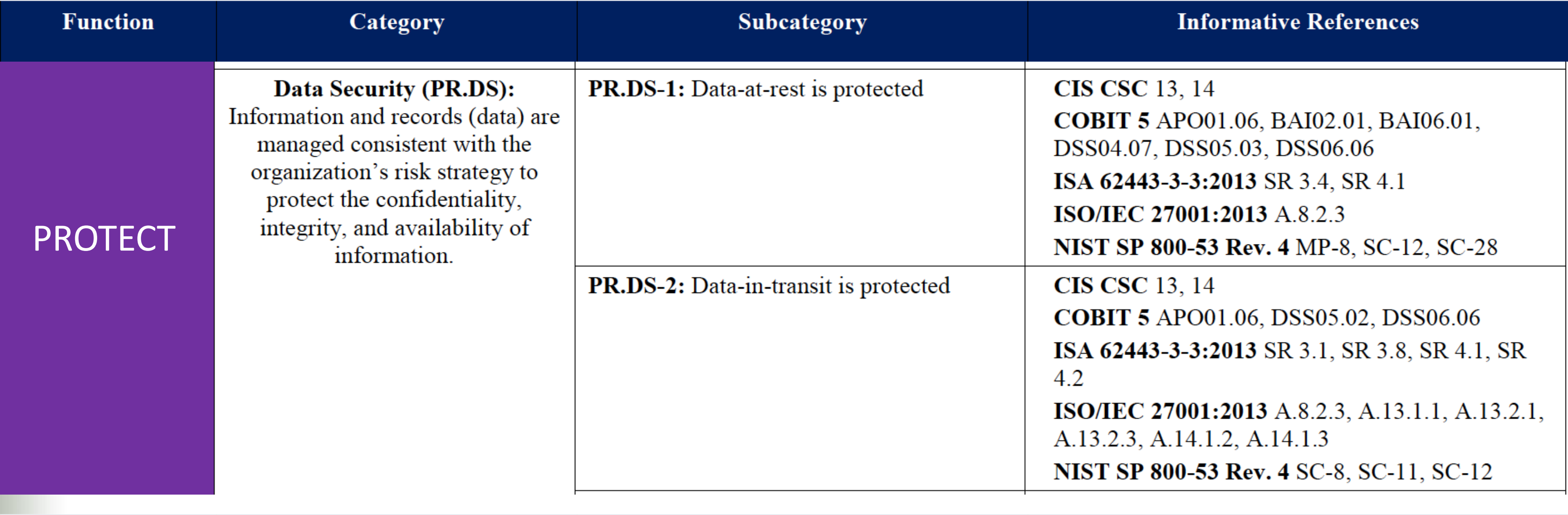
What techniques can contain impacts of incidents?

What techniques can restore capabilities?

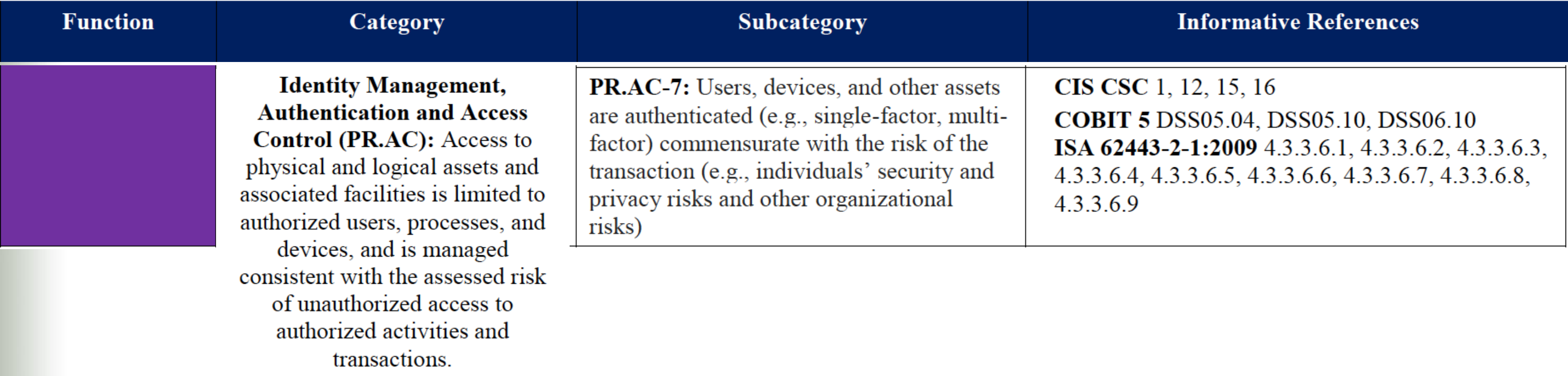
Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management[1.1]
Protect	**Identity Management, Authentication and Access Control**[1.1]
	Awareness and Training
	Data Security
	Information Protection Processes & Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

Core – Example

Cybersecurity Framework Component



Function	Category	Subcategory	Informative References
PROTECT	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	**CIS CSC** 13, 14 **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 **ISA 62443-3-3:2013** SR 3.4, SR 4.1 **ISO/IEC 27001:2013** A.8.2.3 **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28
		PR.DS-2: Data-in-transit is protected	**CIS CSC** 13, 14 **COBIT 5** APO01.06, DSS05.02, DSS06.06 **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12



Function	Category	Subcategory	Informative References
	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-7:** Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9

Sample 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"

Sample Resources

www.nist.gov/cyberframework/industry-resources

Manufacturing Profile

[NIST Discrete Manufacturing Cybersecurity Framework Profile]

Self-Assessment Criteria

[Baldrige Cybersecurity Excellence Builder]

Baldrige Excellence Framework
Baldrige Excellence Framework
Baldrige Excellence Framework

Manufacturing Case Study

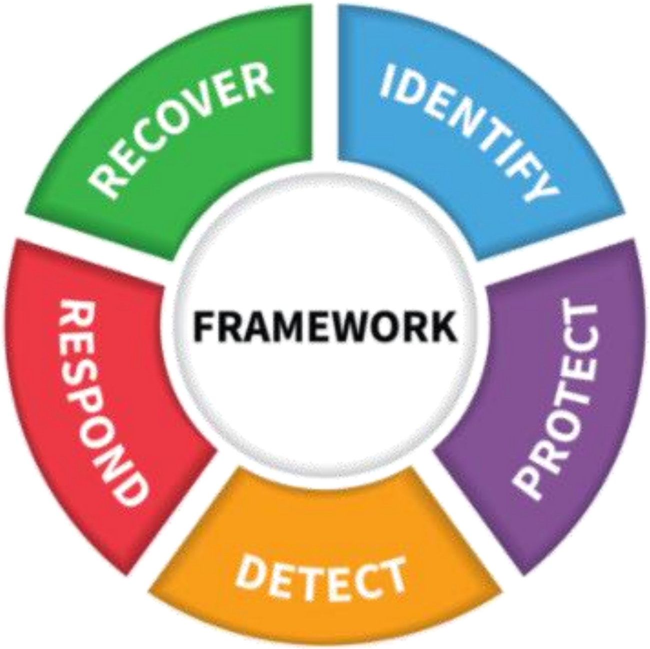
[The Cybersecurity Framework in Action: An Intel Use Case]

Learning More

Framework for Improving Critical Infrastructure Cybersecurity

News and information

www.nist.gov/cyberframework



Learn about the NIST Cybersecurity Risk Management Conference https://www.nist.gov/news-events/events/2018/11/nist-cybersecurity-risk-management-conference

Registration now open at https://www.fbcinc.com/e/NIST/Framework/attendeereg.aspx

Additional cybersecurity resources through

Computer Security Resources Center - http://csrc.nist.gov/

National Cybersecurity Center of Excellence - http://nccoe.nist.gov/

Please direct questions, comments, ideas to cyberframework@nist.gov

"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development (NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674, Fax: 202-459-9673, Email: nco@nitrd.gov, Website: https://www.nitrd.gov