Framework for Improving Critical Infrastructure Cybersecurity

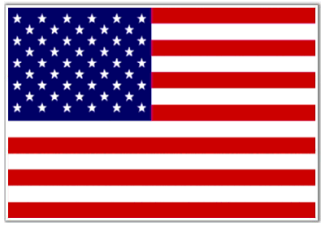
August 2018

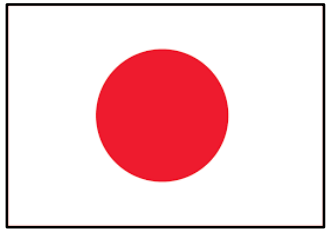
cyberframework@nist.gov

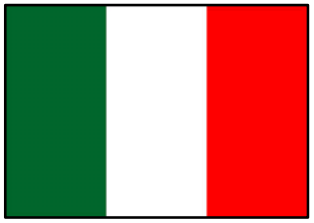
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

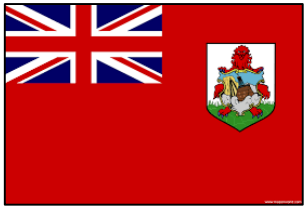
International Use

Framework for Improving Critical Infrastructure Cybersecurity









NTT
NIPPON TELEGRAPH AND TELEPHONE CORPORATION

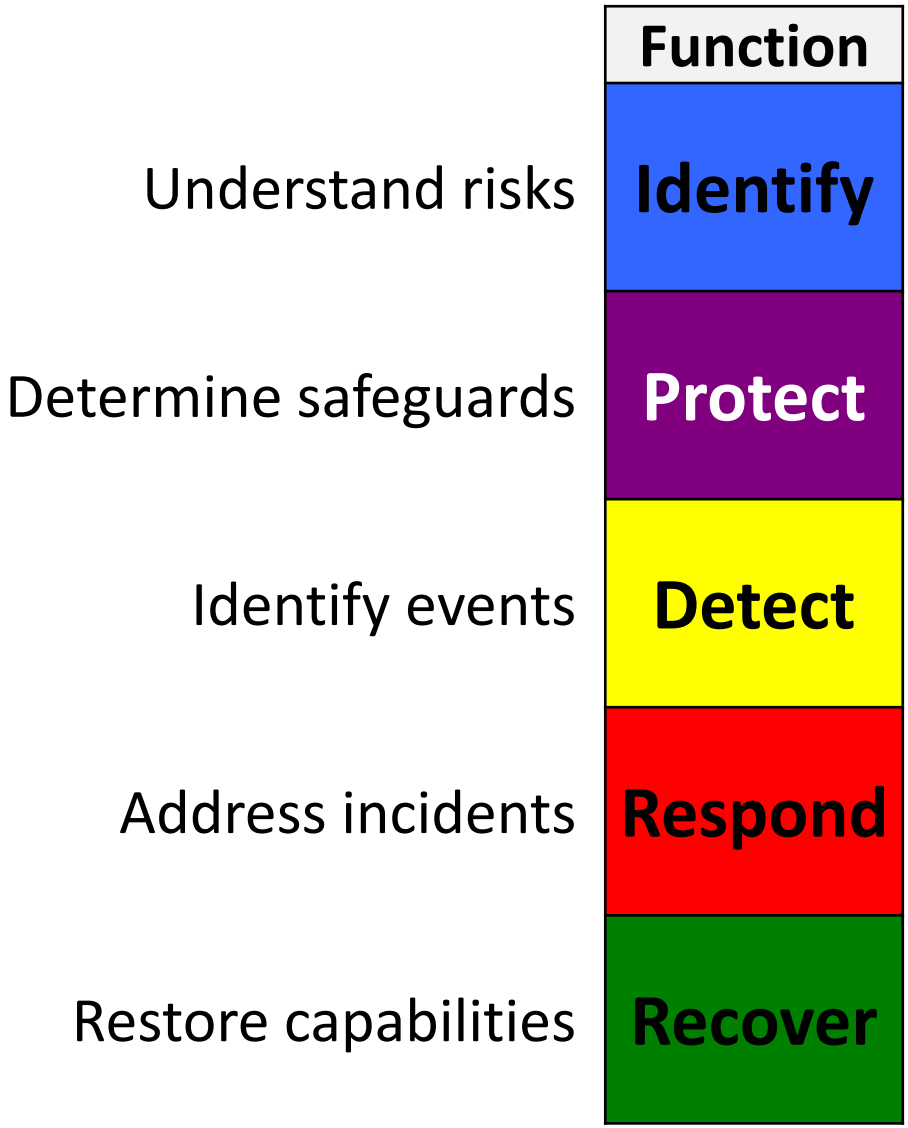
ONTARIO ENERGY BOARD

IMO INTERNATIONAL MARITIME ORGANIZATION

ISO IEC

Core

A Catalog of Cybersecurity Outcomes



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

Core – Example

Framework for Improving Critical Infrastructure Cybersecurity

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident	**CIS CSC** 19 **COBIT 5** APO12.06, BAI01.10 **ISA 62443-2-1:2009** 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	**CIS CSC** 19 **COBIT 5** EDM03.02, APO01.02, APO12.03 **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Incidents are reported consistent with established criteria	**CIS CSC** 19 **COBIT 5** DSS01.03 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8

5 Functions

23 Categories

108 Subcategories

6 Informative References

- Extensible to any reference
- Not exhaustive for a given Informative Reference
- Now piloting Online Informative References

ISO/IEC Technical Report 27103:2018

Information technology – Security techniques – Cybersecurity and ISO and IEC Standards

"This document demonstrates how a cybersecurity framework can utilize current information security standards to achieve a well-controlled approach to cybersecurity management."

https://www.iso.org/standard/72437.html

Threat-Based Profiles

Framework for Improving Critical Infrastructure Cybersecurity

Sub-category	Probable Threats			Priority
	Ransomware	Distributed Denial-of-Service	Botnets	
1		X	X	moderate
2				n/a
3	X	X	X	high
…				…
108		X		low

Key Framework Attributes

Principles of the Current and Future Versions of Framework

- Common and accessible language
- It's adaptable to many technologies, lifecycle phases, sectors and uses
- It's risk-based
- It's meant to be paired
- It's a living document

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