Applying the NIST Cybersecurity Framework: A Primer

Dan Dister
Chief Information Security Officer
State of New Hampshire
June 5, 2018

1

Agenda

- The NIST Cybersecurity Framework (CSF)
  - History
  - Overview
  - CSF Core Functions
  - CSF Functional Categories
  - Applying the CSF
- Practical Cybersecurity
  - Top 10 Ways to Secure Your Computer
  - Good Cybersecurity Habits
  - Resources
- Questions

2

History

- Repeated cyber intrusions demonstrated the need for improved cybersecurity
- February 12, 2013: Executive Order 13636 -- Improving Critical Infrastructure Cybersecurity
  - Objective: Develop a voluntary, cybersecurity framework
- The **National Institute of Standards and Technology (NIST)** developed the "Framework for Improving Critical Infrastructure Cybersecurity" (the "**Cybersecurity Framework**")
  - Input from over 1000 different entities (government, academics, individuals)
- Final version released in February 2014
  - Delivered to critical infrastructure providers and the public
- May 2017: Executive Order 13800 mandated the CSF for all Federal Agencies
- Version 1.1 updated in 2017, published April 2018
  - Added Supply Chain cybersecurity

3

Overview of the NIST CSF

What is the Cybersecurity Framework (CSF)?

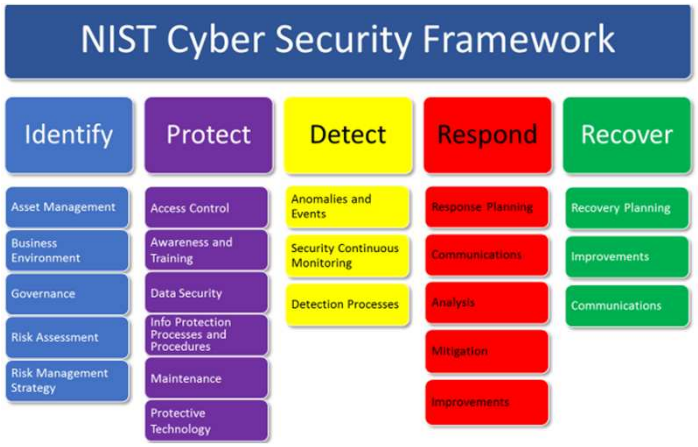
- Includes a set of standards, methodologies, procedures, and processes **that align policy, business, and technological approaches** to address cyber risks.
- Provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure **identify, assess, and manage cyber risk**.
- **Identifies areas for improvement** to be addressed through future collaboration with particular sectors and standards-developing organizations.

But also keep in mind:

- It's a framework, not a prescriptive standard
- Does not tell an organization how much cyber risk is tolerable, nor provide "the one and only" formula for cybersecurity.
- Enable best practices to become standard practices for everyone via common lexicon to enable action across diverse stakeholders.

4

The CSF Core Functions



5

The CSF Functional Categories

Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

6

The NIST Cybersecurity Framework (4)

Applying/Using the CSF:

- Integrate Enterprise and Cybersecurity Risk Management *(strategy)*
- Manage Cybersecurity Requirements *(gaps, tools, capabilities)*
- Integrate and Align Cybersecurity and Acquisition Processes
- Evaluate Organizational Cybersecurity *(Implementation Tiers: Partial, Risk Informed, Repeatable, Adaptive)*
- Manage the Cybersecurity Program *(metrics and measures)*
- Maintain a Comprehensive Understanding of Cybersecurity Risk
- Report Cybersecurity Risks
- Inform the Tailoring Process *(800-53 control selection)*

7

Practical Cybersecurity

- The NIST CSF is great for large organizations
- Probably too difficult to implement for small business or local government
- But – the core principles (Identify, Protect, Detect, Respond, Recover) can translate to anyone at any level

The following slides provide some basic cybersecurity practices

8

Top 10 Ways to Secure Your Computer

1. Connect to a Secure Network
2. Enable and Configure a Firewall
3. Install Antivirus and Antispyware Software
4. Remove Unnecessary Software
5. Modify/Disable Unnecessary Default Features
6. Operate Under the Principle of Least Privilege
7. Secure Your Web Browser (and use a current one)
8. Apply Software Updates
9. Enable Future Automatic Updates
10. Use Good Security Practices

9

Good Cybersecurity Practices

- Improve password security
  - Create a strong password (upper, lowercase, number, special character)
  - Consider using a password manager (LastPass, Dashlane, KeePass, 1Password)
  - Use two-factor authentication, if available
  - Use security questions properly
  - Create unique accounts for each user per device, and for each service
- Keep all of your personal electronic device software current
- Be suspicious of unexpected emails or email from people you don't know
- Also be suspicious of email from people you know, but are "out of character" for that person

10

Resources

- National Institute of Standards and Technology (NIST)
  - Computer Security Resource Center https://csrc.nist.gov/
  - Cybersecurity Framework https://www.nist.gov/cyberframework
- DHS/US-CERT
  - https://www.us-cert.gov/home-and-business
  - https://www.us-cert.gov/publications/securing-your-web-browser
- Center for Internet Security https://www.cisecurity.org/
- Cybersecurity for Small Business (Federal Communications Commission)
  - https://www.fcc.gov/general/cybersecurity-small-business
- Consumer Information on Computer Security (Federal Trade Commission)
  - https://www.consumer.ftc.gov/articles/0009-computer-security

11

Questions?

12

Critical Infrastructure Sectors

- Chemical Sector
- Commercial Facility
- Communications
- Critical Manufacturing
- Dams Sector
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare/Public Health
- Information Technology
- Nuclear Reactors/Materials
- Transportation Systems
- Water Systems

Note: There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. (PPD-21)

13