

Applying the NIST Cybersecurity Framework to Elections

February 2017

Joshua M Franklin

cyberframework@nist.gov

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

Improving Critical Infrastructure Cybersecurity

“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

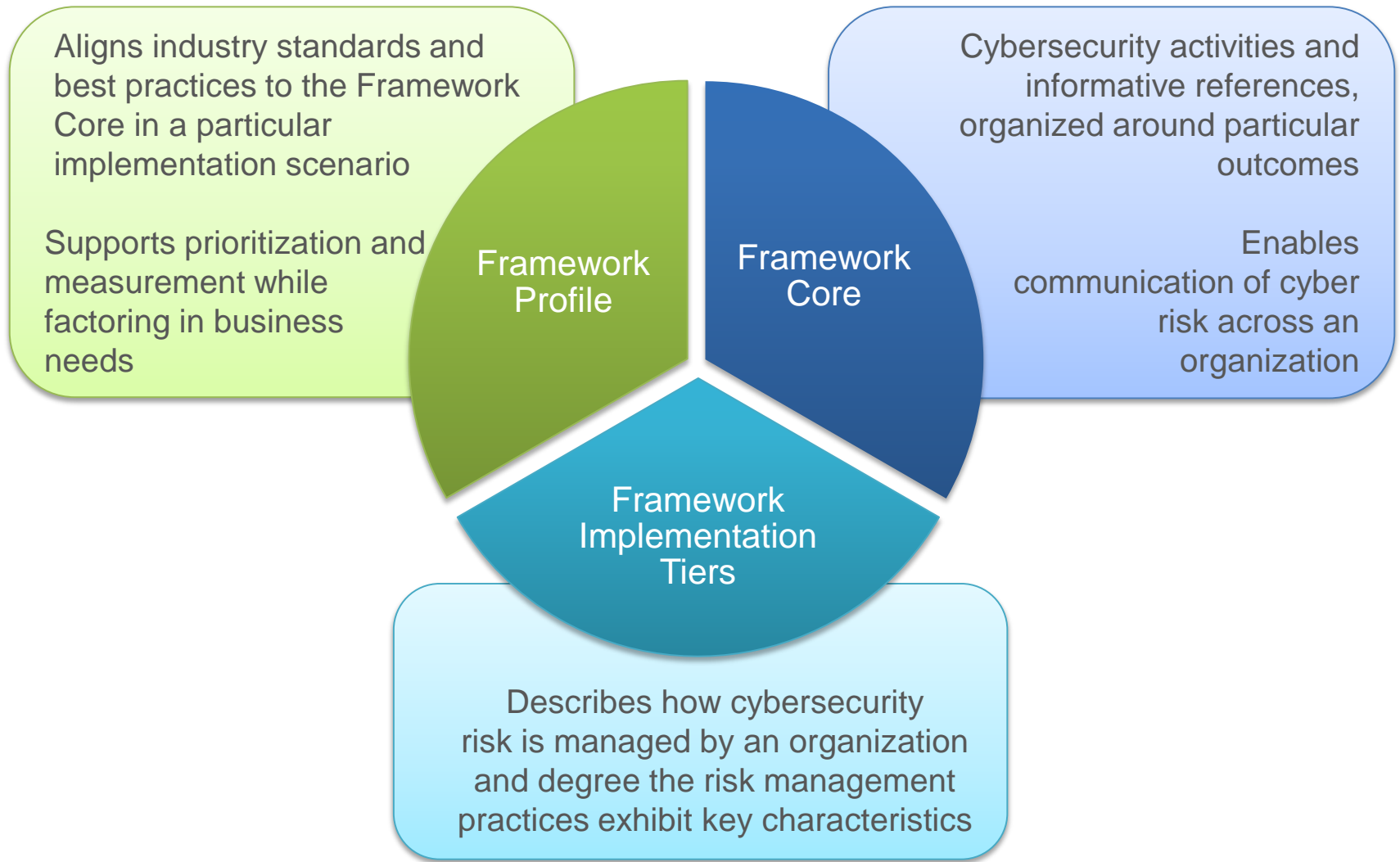
12 February 2013

The Framework Is for Organizations...



- Of **any size**, in **any sector** in (and outside of) the critical infrastructure.
- That already have a **mature** cyber risk management and cybersecurity program.
- That **don't yet** have a cyber risk management or cybersecurity program.
- Needing to **keep up-to-date** managing risks, facing business or societal threats.
- In the federal government, too...since it is compatible with FISMA requirements and goals.

Cybersecurity Framework Components



Core

Cybersecurity Framework Component

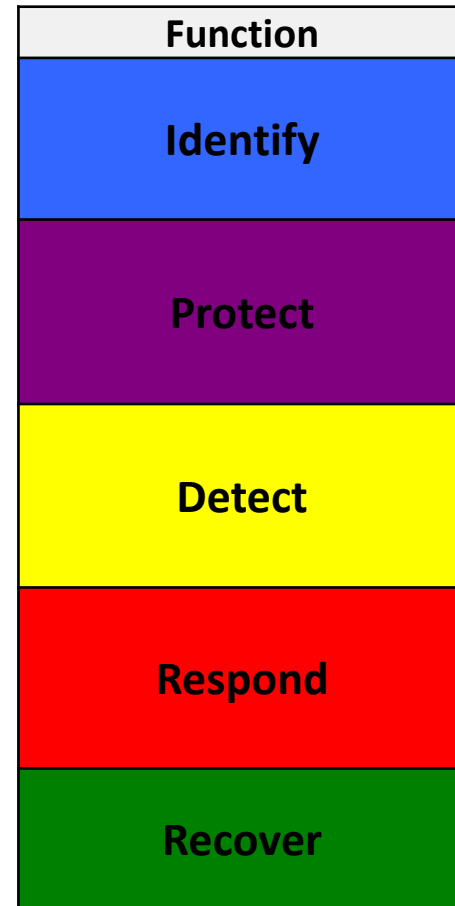
What processes and assets need protection?

What safeguards are available?

What techniques can identify incidents?

What techniques can contain impacts of incidents?

What techniques can restore capabilities?



Core

Cybersecurity Framework Component

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

Core

Cybersecurity Framework Component

Function	Category	Subcategory	References
Identify			
Protect			
Detect			
Respond			
Recover			

Core

Cybersecurity Framework Component

Function	Category	Subcategory	References
Identify	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.		
Protect			
Detect			
Respond			
Recover			

Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

Core

Cybersecurity Framework Component

Function	Category	Subcategory	References
Identify	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	
Protect			
Detect			
Respond			
Recover			

ID.AM-1: Physical devices and systems within the organization are inventoried

Core

Cybersecurity Framework Component

Function	Category	Subcategory	References
Identify	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried.	<ul style="list-style-type: none"> • CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
			<ul style="list-style-type: none"> • CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
Protect			
Detect			
Respond			

Profile

Cybersecurity Framework Component

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

Identify

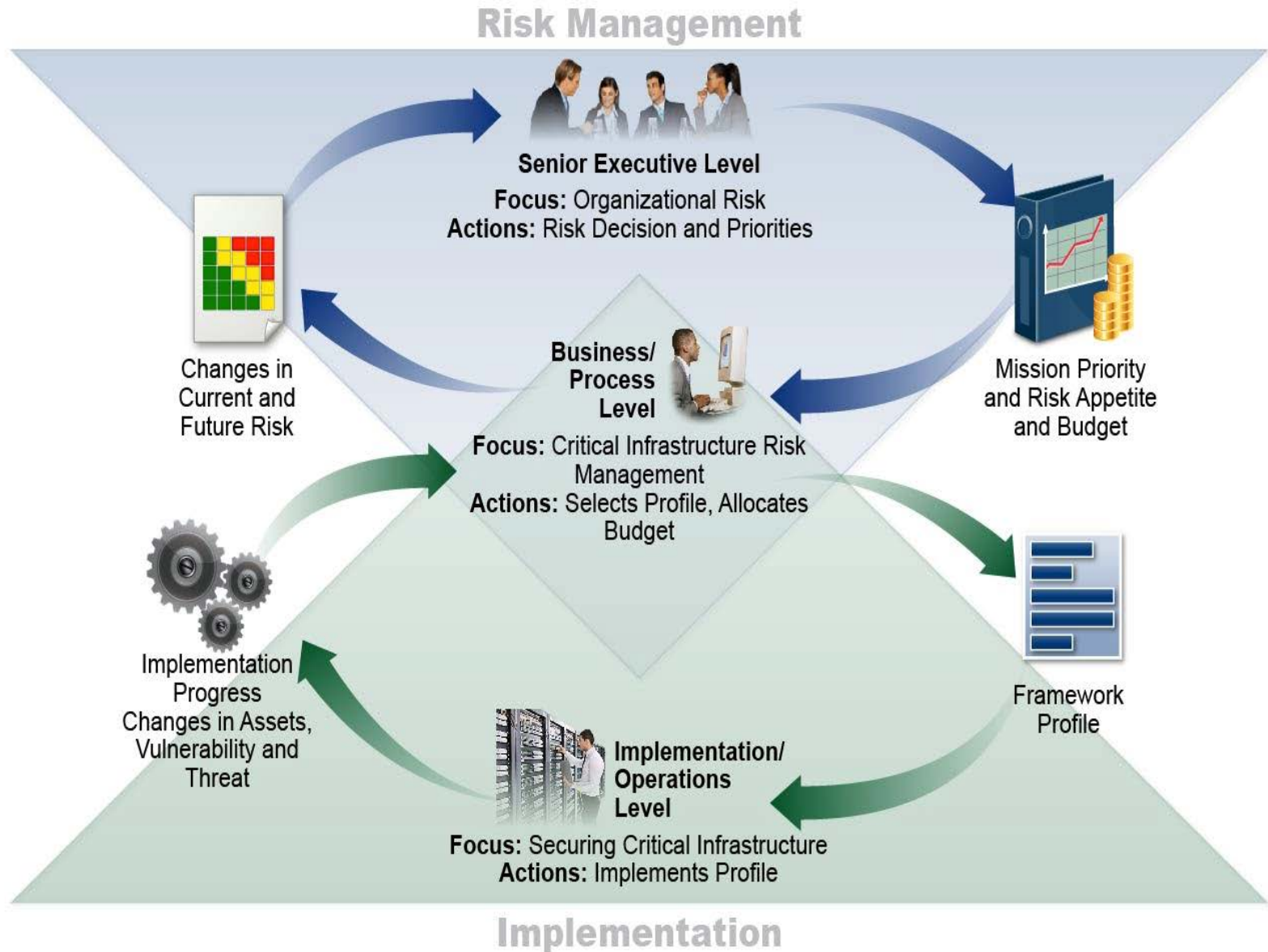
Protect

Detect

Respond

Recover

Supporting Risk Management with Framework



Framework 7-Step Process

- Step 1: Prioritize and Scope
- Step 2: Orient
- Step 3: Create a Current Profile
- Step 4: Conduct a Risk Assessment
- Step 5: Create a Target Profile
- Step 6: Determine, Analyze, and Prioritize Gaps
- Step 7: Implementation Action Plan

Key Attributes

It's a framework, not a prescriptive standard

- Provides a common language and systematic methodology for managing cyber risk.
- Is meant to be adapted.
- 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.

It's voluntary

It's a living document

- It is intended to be updated as stakeholders learn from implementation, and as technology and risks change...more later.
- That's one reason why the Framework focuses on questions an organization needs to ask itself to manage its risk. While practices, technology, and standards will change over time—principles will not.

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](#)



[Energy Sector Cybersecurity Framework
Implementation Guidance](#)

Examples of State & Local Use



Texas, Department of Information Resources

- Aligned Agency Security Plans with Framework
- Aligned Product and Service Vendor Requirements with Framework

North Dakota, Information Technology Department

- Allocated Roles & Responsibilities using Framework
- Adopted the Framework into their Security Operation Strategy



GREATER HOUSTON
PARTNERSHIP

Making Houston Greater.

Houston, Greater Houston Partnership

- Integrated Framework into their Cybersecurity Guide
- Offer On-Line Framework Self-Assessment

National Association of State CIOs

- 2 out of 3 CIOs from the 2015 NASCIO Awards cited Framework as a part of their award-winning strategy



New Jersey

- Developed a cybersecurity framework that aligns controls and procedures with Framework

NIST Manufacturing Profile

[NIST Discrete Manufacturing Cybersecurity Framework Profile](#)

Utilizing CSF Informative References to create tailored language for the manufacturing sector

- NIST SP 800-53
- NIST SP 800-82
- ISA / IEC 62443



NIST Manufacturing Profile In Action

		Maintain Personnel Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals
Category		Subcategories			
Identify	Asset Management	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1
		ID.AM-2	ID.AM-2	ID.AM-2	ID.AM-2
		ID.AM-3	ID.AM-3	ID.AM-3	ID.AM-3
		ID.AM-4	ID.AM-4	ID.AM-4	ID.AM-4
		ID.AM-5	ID.AM-5	ID.AM-5	ID.AM-5
		ID.AM-6	ID.AM-6	ID.AM-6	ID.AM-6
	Business Environment	ID.BE-1	ID.BE-1	ID.BE-1	ID.BE-1
		ID.BE-2	ID.BE-2	ID.BE-2	ID.BE-2
		ID.BE-3	ID.BE-3	ID.BE-3	ID.BE-3
		ID.BE-4	ID.BE-4	ID.BE-4	ID.BE-4
		ID.BE-5	ID.BE-5	ID.BE-5	ID.BE-5
	Governance	ID.GV-1	ID.GV-1	ID.GV-1	ID.GV-1
		ID.GV-2	ID.GV-2	ID.GV-2	ID.GV-2
		ID.GV-3	ID.GV-3	ID.GV-3	ID.GV-3
		ID.GV-4	ID.GV-4	ID.GV-4	ID.GV-4
	Risk Assessment	ID.RA-1	ID.RA-1	ID.RA-1	ID.RA-1
		ID.RA-2	ID.RA-2	ID.RA-2	ID.RA-2
		ID.RA-3	ID.RA-3	ID.RA-3	ID.RA-3
		ID.RA-4	ID.RA-4	ID.RA-4	ID.RA-4
		ID.RA-5	ID.RA-5	ID.RA-5	ID.RA-5
		ID.RA-6	ID.RA-6	ID.RA-6	ID.RA-6

Application to Elections

- No common way to express cybersecurity posture of a jurisdiction
- The elections community could create a CSF profile
 - For large, medium, and small jurisdictions
- Focus on technology **and** procedures
- Who would lead? NASED, EAC, NIST?
- Need broad community involvement

Questions?

Where to Learn More and Stay Current



Framework for Improving Critical Infrastructure Cybersecurity and related news, information:

www.nist.gov/cyberframework

Additional cybersecurity resources:

<http://csrc.nist.gov/>

Questions, comments, ideas:

cyberframework@nist.gov

