Framework for Improving Critical Infrastructure Cybersecurity

January 2016



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"



President Barack Obama
Executive Order 13636, 12 February 2013

Cybersecurity Framework Components

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

Supports prioritization and measurement while factoring in business needs

Framework Profile

Framework Core Cybersecurity activities and informative references, organized around particular outcomes

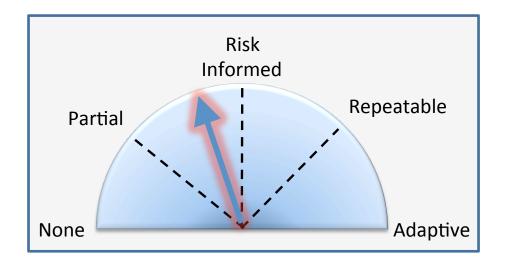
Enables communication of cyber risk across an organization

Framework Implementation Tiers

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

Implementation Tiers

Cybersecurity Framework Component



- Allow for flexibility in implementation and bring in concepts of maturity models
- Reflect how an organization implements the Framework Core functions and manages its risk
- Progressive, ranging from Partial (Tier 1) to Adaptive (Tier 4),
 with each Tier building on the previous Tier
- Characteristics are defined at the organizational level and are applied to the Framework Core to determine how a category is implemented.



Core

Cybersecurity Framework Component

Function	unction Category	
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
	Anomalies and Events	DE.AE
Detect	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
	Response Planning	RS.RP
	Communications	RS.CO
Respond	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
	Recovery Planning	RC.RP
Recover	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References		
ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO01.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11		
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated ID.BE-3: Priorities for	COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.3, A. 15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12		
organizational mission, objectives, and activities are established and communicated	NIST SP 800-53 Rev. 4 PM-8		
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14		
ID.BE-5: Resilience requirements to support delivery of critical services are established	ISO/IEC 27001:2013 A.11.2.2, A. 11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14		

Profile

Cybersecurity Framework Component

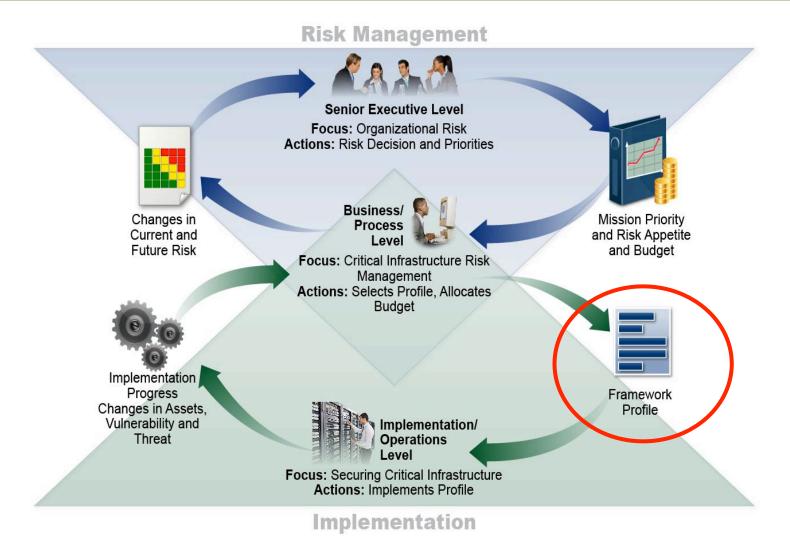
Ways to think about a Profile:

- 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

Using Profiles to Communicate Priorities



Building a Profile

A Profile Can be Created in Three Steps



Mission				
Priority	Objective			
1	A			
2	В			
3	С			



2

Cybersecurity Requirements



Legislation
Regulation
Internal & External Policy
Best Practice

Subcategory
1
2
3
•••
98

Operating
Methodologies

3

Guidance and methodology on implementing, managing, and monitoring

Resource and Budget Decisioning

What Can You Do with a CSF Profile



Sub-			Year 1	Year 2
category	Priority	Gaps	Activities	Activities
1	moderate	small		X
2	high	large	X	
3	moderate	medium	X	
•••	•••	•••		
98	moderate	none		reassess

...and supports on-going operational decisions too

Examples of Industry Resources



The Cybersecurity Framework in Action: An Intel Use Case

Cybersecurity Guidance for Small Firms





Energy Sector Cybersecurity Framework Implementation Guidance

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



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

Framework Roadmap Items

Authentication

Automated Indicator Sharing

Conformity Assessment

Cybersecurity Workforce

Data Analytics



Federal Agency Cybersecurity Alignment

International Aspects, Impacts, and Alignment

Supply Chain Risk Management

Technical Privacy Standards

Ways CSF Can Support RMF

Draft Use Cases

- Use case 1: Supporting SP 800-39 Frame activities with CSF Categories
- Use case 2: Supporting the RMF Categorize step with CSF Business Environment Materials
- Use case 3: Supporting the RMF Select step with a CSF Profile
- Use case 4: Supporting RMF Assess and SP 800-30 Assess with a CSF Profile
- Use case 5: Assessing the State of FISMA-Based Risk Management Practices

Supporting the RMF Categorize Step

Use Case #2 for FISMA-Cybersecurity Framework Combined Use

Architecture Description

Architecture Reference Models Segment and Solution Architectures Mission and Business Processes Information System Boundaries

PROCESS OVERVIEW

Starting Point

Organizational Inputs

Laws, Directives, Policy Guidance Strategic Goals and Objectives Priorities and Resource Availability Supply Chain Considerations

Repeat as necessary



Step 1

CATEGORIZE Information System

FIPS 199/SP 800-60

RISK

MANAGEMENT

FRAMEWORK



Step 2

SELECT Security Controls

FIPS 200/SP 800-53

Step 6

MONITOR Security Controls

SP 800-137/SP 800-53A



Step 5

AUTHORIZE Information System

SP 800-37



Step 4

ASSESS Security Controls

SP 800-53A



Step 3

IMPLEMENT Security Controls

Many SPs



Supporting the RMF Categorize Step

Profile

A sector, subsector, or organization's customization of the Core for their purposes. Aligns, identifies conflicts in organizational inputs, and prioritizes cyber objectives commensurate with mission objectives

ned Use

Organizational Inputs

Laws, Directives, Policy Guidance Strategic Goals and Objectives Priorities and Resource Availability Supply Chain Considerations

Repeat as necessary



Step 6

MONITOR Security Controls

SP 800-137/SP 800-53A



Step 5

AUTHORIZE Information System

SP 800-37



Step 1

CATEGORIZE Information System

FIPS 199/SP 800-60

RISK MANAGEMENT FRAMEWORK

Step 4

ASSESS Security Controls

SP 800-53A



Step 2

SELECT Security Controls

FIPS 200/SP 800-53



Step 3

IMPLEMENT Security Controls

Many SPs



Supporting the RMF Categorize Step

Use Case #2 for FISMA-Cybersecurity F

Architecture Description

Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries

Repeat as necessary



Step 6

MONITOR Security Controls

SP 800-137/SP 800-53A



Step 5

AUTHORIZE Information System

SP 800-37



Category Business Environment (ID.BE)

The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

Step 1

CATEGORIZE Information System

FIPS 199/SP 800-60

RISK MANAGEMENT FRAMEWORK

Step 4
ASSESS
Security Controls

SP 800-53A



Step 2

SELECT Security Controls

FIPS 200/SP 800-53



Step 3

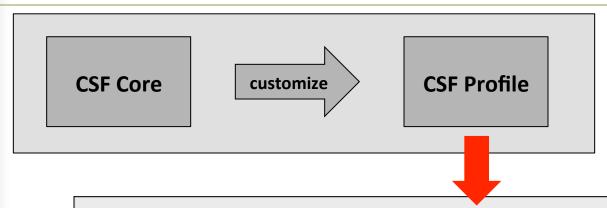
IMPLEMENT Security Controls

Many SPs



Tailoring SP 800-53 Security Controls

Use Case #3 for Risk Management Framework & Cybersecurity Framework



Tailoring Guidance

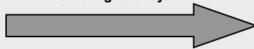
- INITIAL SECURITY CONTROL BASELINE
- (Low, Mod, High)

Before Tailoring

- Toiloring
- __

- Identifying and Designating Common Controls
- · Applying Scoping Considerations
- Selecting Compensating Controls
- · Assigning Security Control Parameter Values
- Supplementing Baseline Security Controls
- Providing Additional Specification Information for Implementation

Creating Overlays



Assessment of Organizational Risk

TAILORED SECURITY CONTROL BASELINE (Low, Mod, High)

After Tailoring



DOCUMENT SECURITY CONTROL DECISIONS

Rationale that the agreed-upon set of security controls for the information system provide adequate protection of organizational operations and assets, individuals, other organizations, and the Nation.

Industry Dialog

Will it soon be time for a Framework update?

What governance models do you believe will work for future Framework maintenance and evolution?

If you have an opinion on these questions (and more), consider responding to our Request for Information -

https://www.federalregister.gov/articles/2015/12/11/2015-31217/ views-on-the-framework-for-improving-critical-infrastructurecybersecurity

Responses due by 9 February at 5PM ET

Resources

Where to Learn More and Stay Current

The National Institute of Standards and Technology Web site is available at http://www.nist.gov

NIST Computer Security Division Computer Security Resource Center is available at http://csrc.nist.gov/

The Framework for Improving Critical Infrastructure Cybersecurity and related news and information are available at www.nist.gov/cyberframework



For additional Framework info and help cyberframework@nist.gov