



The President issued an Executive Order “Improving Critical Infrastructure Cybersecurity,” on February 2013.

The Executive Order calls for the development of a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organizations manage cybersecurity risks.

From this executive order the National Institute of Standards and Technology (NIST) through collaboration between government and the private sector provided a voluntary framework for addressing the advanced persistent threat to the nation’s critical infrastructure.

NASCIO and the National Governor’s Association have been urging states to adopt the NIST Cybersecurity Framework since its release in February 2014.

Components of the Cybersecurity Framework

- Implementation Tiers
 - Organizations Maturity level on risk management
- Framework Core
 - Set of cybersecurity activities, outcomes and references
 - Enterprise Security Policies are based on Framework Core
- Framework Profile
 - Where are we today, roadmap for tomorrow

There are 3 main components of the Cybersecurity framework

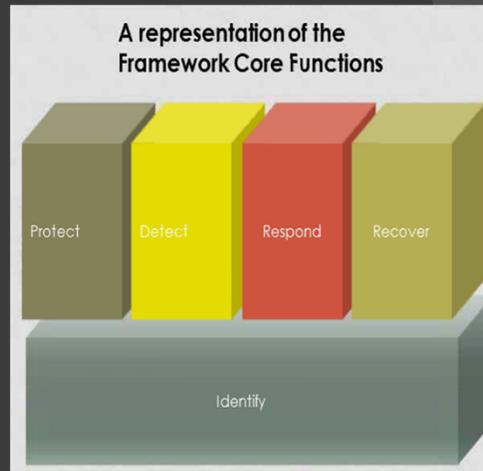
- Implementation Tiers
 - Overview of organizations maturity level on risk management
- Framework Core
 - Set of cybersecurity activities, desired outcomes and references based on existing best practices . Technology neutral.
- Framework Profile
 - Snapshot of today in a given category, roadmap for tomorrow

Our Enterprise Policies are base from the Framework Core

NIST Framework Core

5 Main Functions

- Identify
- Protect
- Detect
- Respond
- Recover



5 Main Functions

February 12, 2014

Cybersecurity Framework

Version 1.0

Table 1: Function and Category Unique Identifiers

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

Identify – Protect – Detect – Respond – Recover

Each Function has a Unique Identifier, and Categories associated with the Function.

***The description for each of these Functions, is also describing each policy. This graphic can be useful when reading through each policy.

Identify –

Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Categories within this Function include: Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy

Protect –

Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
Function supports the ability to limit or contain the impact of a potential cybersecurity event.
Categories within this Function include: Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, Protective Technology

Detect –

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Function enables timely discovery of cybersecurity events.
Categories within this Function include: Anomalies and Events, Security Continuous Monitoring, Detection Processes

Respond –

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Function supports the ability to contain the impact of a potential cybersecurity event.
Categories within this Function include: Response Planning, Communications, Analysis, Mitigation, Improvements

Recover –

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event.
Categories within this Function include: Recovery Planning, Improvements, Communications

February 12, 2014		Cybersecurity Framework		Version 1.0	
Function	Category	Subcategory	Informative References		
IDENTIFY (ID)	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.	ID.BE-1: The organization's role in the supply chain is identified and communicated	<ul style="list-style-type: none"> NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11 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 		
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	<ul style="list-style-type: none"> COBIT 5 APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-8 		
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	<ul style="list-style-type: none"> 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-4: Dependencies and critical functions for delivery of critical services are established	<ul style="list-style-type: none"> 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 		
		ID.BE-5: Resilience requirements to support delivery of critical services are established	<ul style="list-style-type: none"> COBIT 5 DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14 		
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1: Organizational information security policy is established	<ul style="list-style-type: none"> COBIT 5 APO01.03, EDM01.01, EDM01.02 ISA 62443-2-1:2009 4.3.2.6 ISO/IEC 27001:2013 A.5.1.1 NIST SP 800-53 Rev. 4 -1 controls from all families 		
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	<ul style="list-style-type: none"> COBIT 5 APO13.12 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1.1, A.7.2.1 NIST SP 800-53 Rev. 4 PM-1, PS-7 		
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity.	<ul style="list-style-type: none"> COBIT 5 MEA03.01, MEA03.04 ISA 62443-2-1:2009 4.4.3.7 		

Function – Identify

Category – Governance

Subcategory – ID.GV-2: Information Security roles & responsibilities are coordinated and aligned with internal roles and external partners

Information References: A crosswalk to NIST SP 800-53 Rev 4 - PM-1 and PS-7

***PM-1 = Program Management – Information Security Program Plan – Baseline Security Controls

***PS-7 = Personnel Security – Third-Party Personnel Security.

5 Core Functions ties to Baseline Security Controls

APPENDIX A
STATE OF MONTANA
BASELINE SECURITY CONTROLS

Identifier	Family	Class
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

There are 18 Families within NIST 800-53 R4.

FAMILY/Category: Program Management (PM)			
Control Number	Control Name	Priority	Control Baseline
PM-1	Information Security Program Plan	P1	PM-1
<p>The State of Montana:</p> <p>a. Develops and disseminates an organization-wide information security program plan that:</p> <ul style="list-style-type: none"> • Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; • Provides sufficient information about the program management controls and common controls to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended; • Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance; • Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations, organizational assets, individuals, other organizations, and the State; <p>b. Reviews State-wide information security program plan every two years; and</p> <p>c. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.</p>			

FAMILY/Category: Personnel Security (PS)			
Control Number	Control Name	Priority	Control Baseline
PS-7	Third-Party Personnel Security	P1	PS-7
<p>The State of Montana:</p> <p>a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;</p> <p>b. Documents personnel security requirements; and</p> <p>c. Monitors provider compliance.</p>			

These reflect back to the following slide

Subcategory – ID.GV-2: Information Security roles & responsibilities are coordinated and aligned with internal roles and external partners

5 Enterprise Security Policies

- Cybersecurity Core Function:

- 1 – Identify
- 2 – Protect
- 3 – Detect
- 4 – Respond
- 5 – Recover

Enterprise Policy Cybersecurity Core Function 1 - Identify

ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy

A. Maintain an inventory of information system components. Inventory of systems is conducted annually and reviewed for any unauthorized components. Unauthorized components are removed.

B. Map organizational communication and data flows by:

F. Establish and maintain information security policies that provide the following:

G. Identify and document asset vulnerabilities by:

Identify is the Function

Asset Management, Business Environment... is the Subcategory

- A. Maintain an inventory of information system components. – That is Asset Management
- B. Map organizational communication and data flows by – That is Business Environment
- F. Establish and maintain information security policies that provide the following: - Governance
- G. Identify and document asset vulnerabilities by – Risk Assessment

Enterprise Policy Cybersecurity Core Function 2 - Protect

PR	Protect	PR.AC	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

A. Manage identities and credentials for authorized devices and users that:

H. Provide State of Montana personnel and partners cybersecurity awareness education that:

P. Perform remote maintenance of organizational assets in a secure manner by:

- A. Manage identities and credentials for authorized devices and users that – This is access control
- H. Provide state of Montana personnel and partners cybersecurity awareness education that: - Awareness and Training
- P. Perform remote maintenance of organizational assets in a secure manner by – This is Protect – Maintenance

As you are reading these policies, know that they reflect directly back to the Cybersecurity Core Functions.

Consolidation of Enterprise Security Policies

- 6 Total Security Policies
 - 5 Cybersecurity Core Functions
 - Information Technology Security Risk Management Policy
 - Appendix A – Baseline Security Controls
 - Appendix B – Security Roles and Responsibilities
 - The 5 Cybersecurity Core Functions enterprise policies will be posted today on ISAC website for review

There will be a consolidation of Enterprise Security Polices.

We will be moving from 14 Enterprise Security Polices, 5 Enterprise Security Standards to just 6 enterprise security policies. Some of the older polices will become procedures. There will be a document posted before the next meeting showing each of the older polices and where they will reside