Applying Framework to Mobile & BYOD

Framework for Improving Critical Infrastructure Cybersecurity

National Association of Attorneys General

Southern Region Meeting

13 March 2015

cyberframework@nist.gov

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

Cybersecurity Framework

As directed by Executive Order 13636, NIST convened industry to create the Cybersecurity Framework (Framework) for Improving Critical Infrastructure Cybersecurity. Use of the Framework is voluntary.

EO 13636
13 February 2013

→

Workshops & Stakeholder Engagement
Request for Information, Feedback on the Draft &
5 Industry Workshops in 5 Different Cities

→

Framework
12 February 2014

Framework components are used to align

Mission Technology Cybersecurity

10110

The Framework has 3 main components

The Framework is used broadly

International	Federal	State Gov't	Industry
機能	DEPARTMENT OF ENERGY · UNITED STATES OF AMERICA	THE STATE OF TEXAS	intel
Translations	Sector Guidance	State Guidance	White Papers

Learn more and contribute at http://www.nist.gov/cyberframework/

Framework Version 1.0
Related Roadmap Items

Industry Resources
NIST Speaking Engagements

RFI Responses
Frequently Asked Questions

Framework Core

	Functions	Categories	Subcategories	Informative References
What assets need protection?	IDENTIFY			
What safeguards are available?	PROTECT			
What techniques can identify incidents?	DETECT			
What techniques can contain impacts of incidents?	RESPOND			
What techniques can restore capabilities?	RECOVER			

5 Functions 22 Categories 98 Subcategories

Framework Core Excerpt

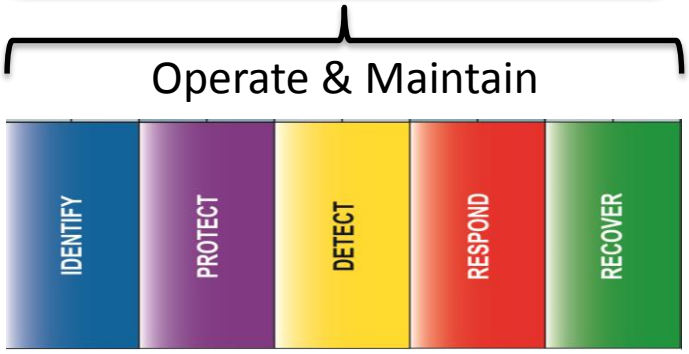
Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	• **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	• **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	• **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	• **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	• **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	• **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	• **COBIT 5** APO13.12 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1 • **NIST SP 800-53 Rev. 4** PM-1, PS-7
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity,	• **COBIT 5** MEA03.01, MEA03.04 • **ISA 62443-2-1:2009** 4.4.3.7

Where Should I Start?

(1) 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.

(2a) 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

(2b) Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.



Framework Version 1.0, Section 3.2, Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance.

Key Questions for New Technologies

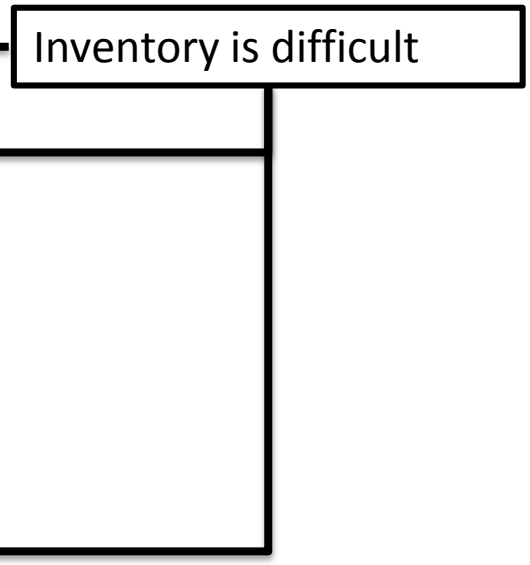
Overarching Question	Question	Who	Decision Materials
Proceed?	Will implementing the technology help me fulfill mission priorities?	Mission	ID.BE-3
	Will implementing the technology adversely affect the mission function of my current systems?	Technology	ID.AM-5
	Will implementing the technology introduce untenable risk?	Cyber Security	ID.RM-2/Profile *Inherent risks*
Proceed now?	Is it possible to implement this technology given my current infrastructure?	Technology	ID.AM-1, 2, & 3
	How can I minimize risk associated with this new technology: • in a way that supports my organization's requirements, and • within my finite budget?	Cyber Security	ID.RM-2/Profile *Inherent risks*
	How much security is 'enough' to implement this new technology?	Cyber Security	ID.RM-2/Profile
Hand-off to operations	What do I need to do to ensure on-going risk management of this new technology?	Cyber Security	*Remaining Categories*

Inherent Risks of Mobile Devices & Bring Your Own Device

- Inventory is difficult
  - Organization-supplied, personnel-supplied, hybrid
- Administrative diligence may be unknown or minimal
  - Patching, software baseline, security configuration management
- Mobile technologies bring increased possibility of malicious code to the enterprise due to increased attack surface and networks
  - Devices tend to connect to a large number of networks, the majority of which are not managed by the organization
  - Lots of spectrum per device (e.g., LTE, WiFi, GPS, Near Field Communication, Blue Tooth)
- Possibility of loosing control of organizational information as it is transported via mobile device
- Risk assessment before ‘go live’ is impossible and impractical
- Strong potential for personal data to traverse organizational networks

Assessing and Minimizing Inherent Risks

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
		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



Assessing and Minimizing Inherent Risks

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
		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

ID.GV-3

ID.GV-1

Personal and organizational data is co-mingled

Privacy Considerations

Framework Version 1.0, Section 3.5, Methodology to Protect Privacy and Civil Liberties

Governance of cybersecurity risk

- An organization's assessment of cybersecurity risk and potential risk responses considers the privacy implications of its cybersecurity program
- Individuals with cybersecurity-related privacy responsibilities report to appropriate management and are appropriately trained
- Process is in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements
- Process is in place to assess implementation of the foregoing organizational measures and controls

Approaches to identifying and authorizing individuals to access organizational assets and systems

- Steps are taken to identify and address the privacy implications of access control measures to the extent that they involve collection, disclosure, or use of personal information

Awareness and training measures

- Applicable information from organizational privacy policies is included in cybersecurity workforce training and awareness activities
- Service providers that provide cybersecurity-related services for the organization are informed about the organization's applicable privacy policies

Anomalous activity detection and system and assets monitoring

- Process is in place to conduct a privacy review of an organization's anomalous activity detection and cybersecurity monitoring

Response activities, including information sharing or other mitigation efforts

- Process is in place to assess and address whether, when, how, and the extent to which personal information is shared outside the organization as part of cybersecurity information sharing activities
- Process is in place to conduct a privacy review of an organization's cybersecurity mitigation efforts

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