DRAFT – Framework Implementation Level Matrix (Function x Role x Level)

		"Levels"		
FUNCTION/ROLE		"1"	"2"	"3"
OVERALL *(worked example on next slide)*				
KNOW	Senior Leader			
	Business Process			
	Operations			
PREVENT	Senior Leader			
	Business Process			
	Operations			
DETECT	Senior Leader			
	Business Process			
	Operations			
RESPOND	Senior Leader			
	Business Process			
	Operations			
RECOVER	Senior Leader			
	Business Process			
	Operations			

DRAFT Overall - Characteristics

	Cyber Levels		
	"1"	"2"	"3"
Overall	• My organization employs a risk assessment methodology to identify its cybersecurity risks. • My organization identifies its internal and external dependencies. • My organization understands its business and mission drivers; laws, regulations, and policy drivers. • My organization has operational situational awareness of the desired and current state of its physical and logical assets.		• Cybersecurity is a precondition to my organization's work and is considered in all business decisions. • My organization's cybersecurity policy is aligned with mission and business objectives, and is used to improve business performance. • My organization dynamically evaluates its security posture and leverages management support to maintain alignment with its stated risk tolerance.

DRAFT Example Recover: Contingency Planning

		Cyber Levels		
Contingency Planning		"1"	"2"	"3"
	Senior Leader	• I'm not sure about redundancy for my critical data.		• There is a clear strategic plan in place for the protection of critical data and essential services.
	Business Process			• My organization not only effectively uses industry-best standards, but we benchmark and meet/exceed industry best practices for redundancy.
	Operations	• My organization's critical data is contained in one location. • My organization has a documented and tested contingency plan.		

DRAFT Know: Asset Management

		Cyber Levels		
Asset Management		"1"	"2"	"3"
	Senior Leader	- I understand the necessity of asset management and assume responsibility for lifecycle accountability.	- Ensure Asset Management Policies are in place.	- I understand how different groups of assets impact the various business objectives. - Ensures resources are available for all aspects of the asset management lifecycle.
	Business Process	-An ad hoc asset tracking process in place. -Legacy assets are removed from network when functionality is superseded.	-A formal asset tracking process is in place with defined periodic revalidation of assets. -Standardized approach exists for network mapping.	- Automated Asset tracking process exists with real time validation and visualization.

DRAFT Know: Asset Management

		Cyber Levels		
Asset Management		"1"	"2"	"3"
	Operations	- Inventory of products exists for my network. -New devices can be added to the network. -I follow guidelines for the removal of assets from the network.	- A map of the current network is available and is stored in a secure manner. - The network map is updated as the network changes. - Wireless devices are included on the network map. - Connections to the cloud, external networks and the internet are included on the map. - I can identify my network assets , the role of each asset, where they reside and who is responsible for them.	-I can identify my high value network assets, the role of each asset, where they reside and who is responsible for them. - Automatic inventory discovery tools are used to discover network devices. - Our organization deploys Dynamic Host Configuration Protocol (DHCP) server logging and utilizes a system to improve the asset inventory and help detect unknown systems through this DHCP information.

DRAFT Protect: Configuration Management

		Cyber Levels		
Configuration Management		"1"	"2"	"3"
	Senior Leader	- I understand that a large number of attacks are due to poor configuration management. - I assume responsibility for a configuration management process.	- Ensure Configuration management Process is in place.	- Ensures resources are available for configuration management process.
	Business Process	- My organization has a configuration and change management process.	- My organization has a formal configuration and change management process.	- My organization uses automated patch management tools. - My organization uses configuration management tools to alert when a configuration changes from the baseline.
	Operations	- A baseline configuration plan is available. - Patches are installed manually in a timely fashion.	- Each version of the configuration is stored for comparative analysis. - Patches are tested prior to installation.	-Proposed configuration changes are reviewed (prior to approval) and documented (once approved). - Automated checking of configurations against baseline to look for unauthorized changes. - Automated deployment of patches across the enterprise.