Comments template for Preliminary
Cybersecurity Framework

Submitted by: __Susan M. Rogers______________________
Date: _____December 13, 2013__________________

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
	Cyberwise CP	Susan M. Rogers		3	162	1.2	The use of risk management, tolerance and appetite are vague and can be expanded slightly to include a broader description of the different types of risk. This will assist in identifying how existing risk activities can be mapped and applied to the NIST cybersecurity framework.	Suggest that the types of risk be added to include enterprise, operational, legal, market, credit etc. Also suggest that this be expanded to define how cyber threat can impact all of these forms of risk, disrupting the market, people, process, technology, external events, legal, market liquidity and systemic risk.
				3	174	1.2	A comprehensive risk management approach to strengthen an organization to survive a cyber threat would include the operational risk process of Business Continuity.	See justification to include Business Continuity references injected into the framework sections: IDENTIFY, PROTECT, RESPOND, RECOVER below.
				3	174	1.2	I participated in the NIST workshops from the vantage point of business continuity, disaster recovery, technology resiliency which can support the goal of preparedness throughout an organization to respond to a cyber-threat. Business Continuity activities that support cybersecurity preparedness are not called out in the framework.	A NIST publication is valued for practical instructions on how to address a complex operational process. I propose that by including business continuity (BC) terminology in the framework sections, NIST will improve the adoption of the framework and significantly expand workforce engagement to build contingency plans that will reduce the impact of cyber threat.
				3	174	1.2	Improved Adoption Rationale	Business Continuity is a mature methodology that exists in most organizations, with clear terminology and process to measure a threat impact and to identify assets, systems, employees, vendors and customers that are most critical and need to be protected.
				3	174	1.2	Improved Adoption Rationale	For small companies, there are affordable ways to adopt a BC program including: affordable or free training, template, tools and a large certified workforce of BC Planners and DR specialists.

Type: E - Editorial, G - General T - Technical

				3	174	1.2	Improved Adoption Rationale	If NIST includes BC terminology in the framework, organizations will have an easier experience communicating how they are meeting components of the framework. The framework can reference usage of Business Impact Analysis, business contingency plans, disaster recovery plans and utilize various levels of crisis communication and event response practices that business teams create under the guidance and structure of their BC programs.
				3	174	1.2	Improved Preparedness Rationale	Citing Business Continuity in the NIST framework will add people into the dialogue that have led their organizations through crisis events such as hurricane Sandy, power outages, network failures etc., and have lessons learned that will enrich cyber event contingency planning.
				3	174	1.2	Improved Preparedness Rationale	Citing BC will encourage information sharing with organizations. Silos may exist that limit the sharing of important information such as: critical asset tracking, impact of emerging risks, contingency plans built through the company critical and single point of failure processes and systems.
				3	183	1.2	Risk based application of process is not well defined. This is important because frameworks cannot be adopted overnight. They take time, with organizations choosing the most important pieces, based on their highest risks, to implement first. Then overtime, more can be adopted.	Suggest that a definition of risk based adoption be added.

				14	466	ID.AM-1	Inventory lists are notoriously hard to keep up to date. More direction is needed to provide small/medium companies help in creating process that is sustainable.	Suggest reference to NIST standards that support identification software development lifecycle, change management, annual disaster recovery (technology), business continuity maintenance and other practices that support refresh of various asset inventories.
				14	466	ID.AM-1	same as above	same as above
				14	466	ID.BE-1	There is opportunity in this section to reference the many sources where business people prioritize and identify impact and emerging risks. This will help with framework adoption.	Reference to practices within Operational Risk, such as a RCSA (Risk and Control Self Assessment), Vendor Management Assessment tools, or Business Continuity BIA, (Business Impact Analysis) can be provided.
				14	466	ID.BE-2	same as above	same as above
				14	466	ID.BE-4	same as above	same as above
				16	466	ID.RA-3	Threats to organizational assets should also be shared to the groups within a company that can put contingencies in place.	add verbiage to share threat information.
				20	466	PR.IP-4	There is an opportunity here to identify the practices within Disaster Recovery that manage back-up strategy, technology recovery and resiliency based on the recovery time objectives and recovery point objectives of critical processes.	Include reference to Disaster Recovery or Business Continuity standards that include DR.
				20	446	PR.IP-9	BC, DR and Incident handling plans may be in place however they may not be expanded to anticipate response and contingency of the impact of cyber threat.	Add verbiage that BC, DR, Incident plans are in place, maintained and include activities to respond to a cyber event, that includes both physical and technology failure and multi-regional impact.
				24	446	RS.CO-5	There is an opportunity to use the phrase "contingency plan activation" and to reference the coordination of response that business teams and technology teams must have in order to mitigate the effects of a cyber event.	Add verbiage that links Info. Sec. Incident Response to the Business Continuity Crisis Response process that would simultaneously stand up to mitigate a significant cyber event.

				25	446	RC.RP-1	The standard states plan recovery for systems and assets affected by cybersecurity. However, all sections within section RC can be strengthened by referencing Business and Enterprise response.	Add verbiage that links technology recovery to business recovery and impact mitigation.