Comments template for Preliminary Cybersecurity Framework

Submitted by: Richard J. Harknett, Jill Wolf, Andrew Douglas, University of Cincinnati
Date: Dec 11, 2013

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	University of Cincinnati	Harknett, et.al.	g				Our main comments below center on improving the connection between the Profile and the Tier sections of the Framework. In particular to the Tiers it is unclear whether they should be presented as descriptive categories or aspirational templates directly associated with developing Current and Target Profiles. As presented now, each Tier is given equal weight, but Tier 1 and 2 are clearly not where we need critical infrastructure to be if the goal is national cybersecurity in CI. Ideally the presentation would be significantly edited to frame the tiers 1 and 2 as examples of Current Profiles that can and should be improved toward target profiles that resemble tiers 3 & 4. The president's EO calls for a framework that has, for example, repeatable outcomes and yet we only get to those in tier 3. The tiers are not equal and the first two should not be presented in a manner in which organizations could choose them as acceptable standards for critical infrastructure. They are descriptions that we need people to develop target profiles to move away from.	
			g	9	328-9	2.4	For example, these lines talk about a tier selection process and that "Organizations should determine the desired Tier." Tier 1 is not a desireable tier from a cybersecurity standpoint, so why would we present it as something that could be chosen?	rewrite this section so that it is tied to profile and higher tiers. "Organizations should determine their current profile relative to the tiers listed below. In instances where their current profile resembles tier 1 and tier 2, target profiles should be established to move the organization toward the cybersecurity practices associated with tiers 3 and 4."

			g	9,10	321-82	2.4	Language needs to be clarified as to whether the tier is to be considered a baseline category, an aspirational category and is aligned with any legal or regulatory standards. The following represents some specific language suggestions:	
			g	9	323-26	2.4		"The Tiers range from Partial (Tier 1 that represents a baseline of activities from which organizations should consider moving via a Target profile) to Adaptive (Tier 4 that represents core practices that enhance cybersecurity significantly)."
				9	332	2.4		"Tier 1: Partial This Tier should be used to guage current practices and serve as a baseline for establishing a Target profile aligned with Tiers 3 and 4."
			g	10	347	2.4		"Tier 2: Risk Informed This Tiershould be used to guage current practices and serve as a baseline for establishing a Target profile aligned with Tiers 3 and 4."
			g	10	358	2.4		"Tier 3: Risk-Informed and Repeatable This Tier represents a minimum standard of practices, policies, and standards to which organizations can align their Target profiles."
			g	10	371	2.4		"Tier 4: Adaptive This Tier represents a standard of practices, policies, and standards to which organizations can align their Target profiles."
			g	10	371	2.4		