Comments template for Preliminary
Cybersecurity Framework

Submitted by: Power Fingerprinting, Inc.
Date: December 13th, 2013

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	Power Fingerprinting, Inc.	Carlos R. Aguayo Gonzalez	T			Appendix A	While one of the overall goals of the framework is to provide a performance-based approach to manage cybersecurity risk, there is a lack of metrics and performance evaluation mechanisms included in the current version of the framework. While providing sound metrics to all the Functions in the framework is a daunting task, there are certain Functions and Categories that could include sound performance metrics. For instance, Detection functions could integrate standard performance metrics such as False-Positive Rate (probability of false alarm), when the detection mechanisms erroneously determine that a cybersecurity event has occurred, or Missed-Detection Rate (probability of missed detection), when a detection mechanism fails to detect a true cyber security event.	Include performance evaluation metrics and evaluation procedures in the functions for which sound quantitative performance metrics are available, such as Detection functions
2	Power Fingerprinting, Inc.	Carlos R. Aguayo Gonzalez	G			Appendix D	It is stated that the "Framework will evolve with technological advances and business requirements". This is a necessary requirement in order to keep up with evolving threats and technology/business landscape. There is, however, no mention of the frequency or the procedure to revise the framework and adapt it to emerging threats and technologies.	Include language in Appendix D: "Framework Development Methodology" to describe the process to evolve the framework in the future and introduce new security capabilities, practices, processes, and standards into it.
3	Power Fingerprinting, Inc.	Carlos R. Aguayo Gonzalez	T			Appendix C	With thousands of new incidents, vulnerabilities, and zero-day attacks discovered every year, as well as the emergence of Advanced Persistent Threats, it is important to highlight the importance of the Detect function within the framework. For this reason, detection technology should be highlighted as one of the critical areas for improvement in the cybersecurity framework, similar to Data Analytics and Supply Chain Risk Management. It is important to emphasize Detection Technology in the framework in order to get organizations responsible for critical infrastructure to realize that preventive measures can be breached with certainty by a determined, well-funded adversary.	Include Detection Technology as one of the areas for improvement in Appendix C.

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