Response to Request for Comments of NIST, for Cyber Security Framework published at:
http://www.nist.gov/itl/cyberframework.cfm

From: Ragu Nathan, System Security Consultant, Gaithersburg, Maryland

To: csfcomments@nist.gov

Date: December-11-2013

Subject: Preliminary Cyber security Framework Comments

My comments are as follows:

(1)
Comment on “Figure-1 Framework Core Structure and the associated text”:

The word 'category' has been used by NIST in earlier documents for 'security categorization'; Hence use of an alternate word like 'Outcome Group' and 'Outcome Sub-Group' as opposed to 'categories' and 'Sub categories' will help a lot.

REF: "FIPS Publication 199 Standards for Security Categorization of Federal Information and Information Systems"

(2)
Comment on “Figure-1 Framework Core Structure and the associated text”

The functions IDENTIFY, PROTECT, DETECT, RESPOND and RECOVER are quite clear. As a system security practitioner, I was hoping to see 'categorization based on security impact' to be mentioned some place explicitly. It seems to be not there. In other words, should the framework not explicitly state that the functions are to be implemented in proportion to the SECURITY IMPACT of an organization’s systems?

(3)
Comment on “2.2 Framework profile”

In section 2.2 Framework profile explains 'current' and 'target' profiles.
As one continues to read Section 2.3- Coordination of Framework Implementation it is not too clear where the current vs. target GAP identification falls under.

(4)
Comment on “2.4 2.4 Framework Implementation Tiers”

In section “2.4 2.4 Framework Implementation Tiers” the 'Maturity Level' is being addressed.

The sentence “Framework Implementation Tiers (“Tiers”) describe how an organization manages its cyber-security risk”

Instead should read as:

“The Framework Implementation Tiers (“Tiers”) describe how well an organization manages its cyber-security risk”