From: **Tristan Madani**
Date: Tue, Feb 28, 2017 at 6:25 AM
Subject: Comments about the Cybersecurity Framework Draft Version 1.1
To: cyberframework@nist.gov

Dear Sir or Madam,

First of all, I would like to thank you for your intensive and productive work on the **NIST Cybersecurity Framework**.

I really appreciate your approach, the framework is very effective and has a high degree of reliability.

However, I would recommend to add the two new functions listed below:

- **VERIFY (VE)**
- **CONTINUOUS IMPROVEMENT (CI)**

Some of the tasks I mention in these two new functions are already covered in the framework as subcategories of other functions, but I think that my approach is more clear and also redress the balance between the "defensive" security and the "offensive" security as both must be widely considered.

To make it short, here is how the core framework will looks like:

- **IDENTIFY (ID)**
- **PROTECT (PR)**
- **VERIFY (VE)**
  - Actively verify; the compliance, level of security and effectiveness of protections
  - Organize on a regular basis both internal and external (outsourced, starting in "Black Box" mode) sophisticated penetration tests
  - Organize frequent "Red Team vs Blue Team" exercises, exhaustively describe TTP (Tactics, Techniques, Procedures) of both teams
  - Write advanced attack/defense scenarios based on real world experiences and all identified weaknesses (improving DE and RS functions and helping to re-evaluate ID-RA-6 and RS.AN-2)
  - Evaluation of the adaptation capacities in the event of cybersecurity incidents
- **DETECT (DE)**
- **RESPOND (RS)**
- **RECOVER (RC)**
- **CONTINUOUS IMPROVEMENT (CI)**
  - Technological watch: Closely monitor technological developments
  - Continuous and close follow-up of new vulnerabilities and prioritize them
  - Review the governance and risk management processes to address new cybersecurity risks
  - Improve continuously all internal security policies and methodologies
  - Re-evaluate and adapt response plans, recovery plans to incorporate experiences, both internal and external contexts, new threats and possible cyberattacks
  - Re-evaluate and adapt hardening guides and other technical documentation to follow the technological developments
  - Re-evaluate and develop new methodologies for the analysis of new cybersecurity risks and vulnerabilities

I would also suggest the four following new subcategories regarding the existing functions:

- ID.BE-6 (Business Environment) : SLA are defined together with the management and the business
- PR.DS-9 (Data Security): When possible, use proven cryptography safeguards for confidential data

- PR.DS-10 (Data Security): A security policy for mobile devices is developed and incorporate appropriate security principles
- PR.IP-13 (Information Protection): A patch management policy is developed and implemented

Please do not hesitate to share your thoughts about this proposal.

Thank you very much.

Yours faithfully,

Tristan Madani