From: Yavor Atanasov
Sent: Thursday, March 2, 2017 2:47 PM
To: cyberframework
Subject: Comments - Cybersecurity Framework Draft Version 1.1

Dear NIST team,

Following the issuance of the draft of the Framework for Improving Critical Infrastructure Cybersecurity , v1.1, please find bellow my comments:

1. The framework is incomplete as evidence by the:
a. Missing permanent and periodic controls structure within the framework. It is my opinion that it must be independent group. There a definition must be included for the independence of the security, compliance and audit functions. In addition to that the trivial principles for the Least Privileges, Segregation of duties and Four eyes principle to be defined
b. Critical Information Infrastructure is not defined, the definition of the Critical Infrastructure is generic… however that does not address the accumulation of risk with interconnected hyper converged information systems.

IDENTIFY (ID)
a. ID.BE-4: Change the wording from established to identified
b. Missing periodic gap analysis for Business alignment between resilience needs by the business and the resilience capabilities by the underlining security systems and devices.

PROTECT (PR)
a. The definition of Endpoint protection is missing
b. Third party risk assessment is not considered
c. Environment risk study is not considered
d. Define Security assurance plans, mandatory security clauses within third parties contracts is missing.
e. Establishment of KPI indicators to monitor security for third parties is missing

DETECT (DE)
a. DE.AE-1: Baseline definition should be broadened, to include behavioral patterns including third parties and providers (as they are referenced in the detection process later)
b. Hardening baseline definition of information systems is missing
c. Attack surface and Attack vectors are not defined

RESPOND (RS)
a. Proactive preparedness is not defined (reaction plans to trivial threats like DDoS, Malware and etc… must be created first and validated by the responsible stakeholders
b. Communications: The word “consistent” is open to interpretation; “according” seems more suitable.
c. Communication with regulatory must be independent step
d. RS.MI-3: The section regarding the risk acceptance is weak, as proper risk assessment must be done prior to accepting it.

--
Kind Regards
Yavor Atanasov
Frankfurt am Main, Germany