From: **Sinha Associates**
Date: Mon, Apr 10, 2017 at 4:35 PM
Subject: Sinha Associates Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity
To: cyberframework@nist.gov

In response to NIST seeking public comment on draft Framework Version 1.1 and the following questions, I would like to submit my comments for review.

-Are there any topics not addressed in the draft Framework that could be addressed in the final?

The cyber framework does not include digital risk monitoring such as identifying, and categorizing internet exposed assets as a clear requirement. Mining internet exposed devices, websites, apps, social profiles is a common vector of attack and often times organizations have little visibility as to what is associated to them or their partners or supply chain online. Often time dependencies in websites such as analytical code or login pages are also vectors, but solved with the same method of organization of online facing infrastructure. This is also a neglected facet in the industrial, energy, manufacturing and water sectors as relates the above mentioned digital properties but also SCADA equipment.

An additional industry is now emerging that is categorizing this data on internet scale so as to expose what is associated with these internet facing websites. The Forrester WaveTM: Digital Risk Monitoring white paper was published on Sept 29th 2016 (It can be downloaded here https://www.riskiq.com/white-paper/riskiq-named-leader-digital-risk-monitoring/).

Abandoned websites and domains are a prime example of the type of infrastructure that can be associated with an organization, and is often time a vector for common attacks. Tools are easily available (including google) that allows for providing due diligence on an organizations internet exposed digital presence, of which good hygiene is an important step.

Therefore, we would like to categorization of internet facing assets and external dependancies such as websites, plugins, saas objects included as items to protect in the document as it applies to Framework Core Structure.

2) Based on this update activities in Roadmap areas and activities in the cybersecurity ecosystem are there additional areas that should be added to the Roadmap?

Additional areas that should be included in the roadmap areas particularly as relates with cyber supply chain risk management needs, is the evaluation and categorization of public internet facing domains, apps, devices, saas and infrastructure. This helps to identify easily whether a supply chain partner organizes their digital and internet facing presence without being overly invasive as if a device, code or other brand associated item exists on the internet it should be claimed or identified.

Additional discussion of methodologies can be found in the report mentioned above but also found here https://www.riskiq.com/white-paper/riskiq-named-leader-digital-risk-monitoring/).

Thank you for taking the time to receive my comments.

Please let me know if there is any additional information you may need.

Best Regards,
Sonny Sinha
Principal
Sinha Associates LLC