SECUILIBRIUM
Balancing Information Security and Business Needs

Secuilibrium, LLC • 3800 N Lamar Blvd #730-314 • Austin, Texas 78756 • United States

October 28, 2013

Information Technology Laboratory
ATTN: Adam Sedgewick
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Via email

RE: Preliminary Cybersecurity Framework Comments

Dear Mr. Sedgewick:

I have studied the Preliminary Cybersecurity Framework (PCSF) and appreciate the effort that has gone into it! I would like to submit the following comments for your consideration:

1. General Comment on Framework Core:

   I suggest considering the alternate proposal provided by Phil Agcaoili at http://www.tripwire.com/state-of-security/regulatory-compliance/phil-agcaoili-nist-framework/ in favor of the current framework in the PCSF, for the following reasons:

   a. The list of controls (categories and subcategories) appears to be more comprehensive than the one in the PCSF, and the language used – at least in a number of instances – appears to be more aligned with existing standards that consumers might already be used to.
   b. The matrix reference to existing standards in Agcaoili's proposal is both more comprehensive (covers more existing standards) and easier to navigate (one column per standard).
   c. For the most part, the level of detail in Agcaoili's proposal appears more appropriate to me. For example, prescribing risk assessments on a high level, yet with enough detail to ensure that likelihood and impact of realized threats are considered separately, and then referring to applicable sections in existing standards (as under Assessments in Agcaoili's proposal) seems more approachable to me than awkwardly splitting up the process of risk assessment into the five ID.AM-* subcategories currently in the PCSF).
   d. It seems more appropriate to me to integrate privacy controls into the general framework, rather than to list them in a separate Appendix as in the PCSF.
   e. The spreadsheet presentation of controls makes it easier for organizations to process, adopt, and implement the framework.

2. As a result of my first comment, I will not comment further on the categories and subcategories described in the PCSF. Comments on other parts of the standard are attached in the suggested Excel format.

Please do not hesitate to contact me with any questions!

With kind regards,

David Ochel
Principal
Secuilibrium, LLC
Phone: +1-512-696-1404
Email: david@secuilibrium.com

Enclosures