March 9, 2013

diane.honeycutt@nist.gov,

Adam.Sedgewick@nist.gov

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Re: Comments on Cyber Security Framework

As part of the open public review and comment process on the Cyber Security Framework, I am submitting the following comments to help identify, refine, and guide the many interrelated considerations, challenges, and efforts needed to develop the Framework. The comments offered span the following Specific Industry Practices:
Asset identification and management: Safeguarding Proprietary Information
Monitoring and incident detection tools and capabilities: Management of Technical Debt and Static Analysis Tool Output Post Processing
Mission/system resiliency practices: Resiliency and Public Policy

Current Risk Management Practices

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?
Under Specific Industry Practice: Asset identification and management
It is time to end the indiscriminate use of the Internet for information the organization cannot afford to lose and doesn't know how to protect.
It is time to ask acquisition program managers and industry executives to exercise due diligence and to supply evidence of safeguarding proprietary information based on rational conditions for Internet use and various degrees of urgency.
Safeguard Proprietary Information, http://youtu.be/ADEi3GLmrvA

2. a. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?
Under Specific Industry Practice: Mission/system resiliency practices
There is a lack of a system of system resiliency protocol for anticipating, avoiding, withstanding, mitigating, and recovering from the effects of Cyber adversity whether manmade or natural under all circumstances of use.
Specific engineering, process, and management capabilities needed to implement the system of system resiliency protocol include distributed supervisory control, coordinated recovery time objectives, digital situation awareness, interoperability of information and data, operation sensing and monitoring.
Dependent capabilities prerequisite to fielding the system of system resiliency protocol include a commitment to resiliency within the critical infrastructure and defense industrial base, security in

depth best practices, business process continuity best practices, and system survivability best practices.
The following ordered collection of short YouTube presentations elaborate on the need for Resiliency and Public Policy:

Summary, http://youtu.be/y08UYV_EFso
Challenges, http://youtu.be/PMwgwE9vBZ4
Resiliency Dimensions, http://youtu.be/EIcKdgJ4p2c
Maturity Framework, http://youtu.be/4fWnVhNrxVU
Public Policy Measures, http://youtu.be/bn2N2yeFEx0
Outcomes, http://youtu.be/qPdbpmvqrcc
Silent Slides Set, http://youtu.be/hHFXXWKewJg

2. b. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?
Under Specific Industry Practice: Monitoring and incident detection tools and capabilities
There is a lack of Cyber Security Technical Debt Management tools spanning the organizational, project, or engineering neglect of known good Cyber Security practice that can result in persistent public, user, customer, staff, reputation, or financial loss.
The following ordered collection of short YouTube presentations elaborate on the Management of Technical Debt.

Technical Debt, http://youtu.be/1z6LPnRL4wU
A Finer Edge, http://youtu.be/SDlaMgs-oi0
A Hole in Your Canoe, http://youtu.be/nf26b-toaNA
Assessment, http://youtu.be/9CDnMWO4Sf4
Triggers and Analytics, http://youtu.be/JQPxReIMl-s
Propagation and Cascading, http://youtu.be/6LfKfJ80SYg
Software Malpractice, http://youtu.be/CW7I_Nxf7d8

2. c. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?
Under Specific Industry Practice: Monitoring and incident detection tools and capabilities
There is a need for commonality and interoperability of Static Analysis tool vendor findings output post processing.
There is a need for understandable, usable, and sharable collection of actionable findings that distinguish quality and Cyber Security issues, postulate consequences, segregate likely false positives, and offer triaged presentation of results based on user supplied criteria.

Best Regards,

Don O'Neill
Independent Consultant

Former President (2055-2008)
Center for National Software Studies

ONeillDon@aol.com

301 990-0377