Comments on "Developing a Framework To Improve Critical Infrastructure Cybersecurity"

John Pescatore, SANS Director of Emerging Security Trends

The RFI summary states:

> *"The National Institute of Standards and Technology (NIST) is conducting a comprehensive review to develop a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework" or "Framework"). The Framework will consist of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."*

I have focused my comments on the elements and goals of the Framework listed in that last sentence:

1. **Standards** - there are no shortage of existing security standards, frameworks and compliance regimes. FISMA, PCI, HIPAA, ISO 27001, etc are widely used, available and provide voluminous coverage of thousands of individual security controls.

   Recommendation: The US Government effort does not need to develop new or more standards. If it does so, it will not contribute to any decrease in risk – it will only cause increased diversion of security spending from protection to reporting.

2. **Methodologies/procedures/processes** – the reality is that each business or government agency uses a myriad of individually tailored security methodologies, procedures and processes. However, here are common elements across those that tend to line up with the "biggest bang for the buck" security controls – the Pareto Principle at work. Examples of industry accepted methodologies that have produced definitions of those common controls include the Critical Security Controls, the Payment Card Industry Prioritization Guidelines, the Australian "Strategies to Mitigate Targeted Cyber Intrusions," etc. These methodologies provide very useful mechanisms for prioritizing expenditures and assuring initial security baselines of threat prevention – without doing so, any measurement (let alone reduction) of risk is not possible.

   Recommendation: The Framework effort should focus on supporting and promulgating some definition of common, critical, core security processes and identifying ways the Government can help remove the barriers to more effective implementation. The Government can play a major role in defining maturity levels of these critical processes, and using the market power of the government to drive suppliers of critical infrastructure services to higher levels of maturity. The Framework effort should **not** produce yet another exhaustive catalog of individual methodologies, procedures and processes.

3. **Aligning policy, business, and technological approaches to address cyber risks –** similar to (2) above, the reality is that each business or government agency uses a myriad of individually tailored approaches for defining risk and aligning investments in technology and security. However, what is lacking is some agreed upon common definitions of evaluating if the actual deployed technology and critical systems end up actually vulnerable to attack – regardless of risk estimation.

   Recommendation: Building on the recommendation in (2) above, the Framework effort should focus on developing guidance to auditors and Inspector Generals for evaluating the maturity levels of critical security processes to provide common mechanisms for independent assessment of process risk. Combining auditor/IG process maturity assessment with continuous monitoring of critical security controls to assure basic threat resilience is maintained will lead to dramatic improvements in security in Critical Infrastructure Systems, and support focusing security resources on security not reporting.

Summary Comments: One Critical Infrastructure **not** mentioned in 42 U.S.C. 5195c(e), is the Food Supply, but I think that provides the best analogy to what is needed to increase cyber security. There are no standard standards, methodologies, processes or procedures for a steak dinner, but there **are process maturity standards** for safe handling and storage of food. There **are inspection regimes** in place (often underfunded) to check on the safety and security of the food chain as products move from farms to processors to stores to consumers to assure that basic hygiene is maintained. Cyber security is based on reducing the risk of software, and software is produced and consumed across an ecosystem that is not unlike the Food Chain!