Comments for Preliminary Cybersecurity Framework (Retrieved on 11/21/2013)

Overall Observation:

Similar to other NIST 800 series documents, this document is not based on any academic information assurance model.

Detailed Comments:

Information assurance, cybersecurity, or information security, whatever your favorite term may be, has three key goals: confidentiality, integrity, and availability. Organizations address these goals by using three types of tools: technology, policy and process, and people. This model of Information Assurance was first published by Maconachy, Shou, Ragsdale, and Welch in 2001 (See: http://it210web.groups.et.byu.net/lectures/MSRW%20Paper.pdf). Though other models exist, this is a widely accepted and used model in Information Assurance education since 2005. A key strength of this model is its emphasis on people controls – or the management of the behavior of people for the purposes of information assurance. This perspective makes enterprise security governance a key factor of success.

Sources of threats are also three types: technology, policy and process, and people. In addition, they can be external or internal to the organization.

Two key factors which should drive an enterprise security governance strategy are: organizational mission and risk management (which includes both negative risks – which result in loss; or positive risk – which result in gain).

Making a model such as Maconachy et al. (2001) a foundation will allow risk management and mission related guidance from NIST such as NIST 800-37 and NIST 800-39 to be incorporated into the model and make the strategy a comprehensive enterprise information security governance strategy.

In most organizations, one must also recognize that an enterprise information security governance or risk management strategy will impact the organizational governance strategy heavily. Hence key top executives of the organization must buy into the strategy and support it. In addition, the Chief Information Officer or the Chief Information Security Officer (the key executive in charge of the security governance strategy) must be sufficiently empowered and supported to implement the strategy – and dramatic organizational changes may be required to make this happen in about 50% of US organizations.

Once the above foundational elements have been identified in the opening chapters of the framework, these elements need to permeate the entire discussion of the Cybersecurity Framework document. This will make the proposed Cybersecurity Framework a much more holistic and practical framework. It will also show organizations why a comprehensive strategy is important.

Right now, the lack of a theoretical foundation makes the framework weak. It looks like another NIST document, which by itself does not solve or clarify anything; rather creates another potential compliance burden which will cause additional costs to organizations without improving security behavior. Security culture components and the need to develop a security culture are also starkly absent from the framework.

By citing an information assurance model, the framework can clearly identify which portions of the model (or which security goals) it is able to address so that consumers of the model are fully aware of its scope. It will also strengthen the framework by informing organizations what portions of an information assurance model the framework is addressing. For example, is the framework addressing external threats only and providing a policy and process solution? Is the framework intended to supercede all other NIST documents? If not, why not? A Cybersecurity Framework should be comprehensive enough by itself and should obviate the need to consult a myriad of other documents, standards, and frameworks. Identiying the scope of the Cybersecurity Framework will allow organizations to be clear on what additional frameworks it may need for a comprehensive strategy.

Thanks for the opportunity to comment.

-**Mansur Hasib, D.Sc, CISSP, PMP, CPHIMS**