Comments template for Preliminary
Cybersecurity Framework

Submitted by: ___IDA(Graeme Douglas)
Date: ___13 December 2013

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	IDA	Graeme Douglas	G				The framework may be considered either too simple to be of value, or too large to be economically implemented by many organizations. The impression of the reader depends upon whether Appendix A is read as inclusive of the framework definition or not. The framework is extremely flexible. The extreme flexibility will make it difficult to compare one framework implementation to another, or to correlate framework implementation levels between organizations. Many organizations will not find the framework a useful guiding construct as all elements, in Appendix A, appear to have the same priority. Equally, an organization can do very little and still claim to be compliant with the framework. The framework described in the main body of the text is so simple that it offers little guidance to the prospective implementing organization. On the other hand the very large table, contained in Appendix A, could easily overwhelm or discourage an organization as a wealth of controls is mapped into the framework. This is the first time the categories and sub-categories are introduced in detail. There is a substantial body of work supporting the proposition that significant gains in improving the cybersecurity risk profile of many organization’s simply through the implementation of basic cyber-hygiene.	Identify key elements of the framework, which are mandatory for an organization to be considered to have "implemented" the framework. Basing these minimal requirements on a commonly agreed critical set such as the Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC). Include this in the main body of the text. Explain carefully in the text how the more comprehensive description in Appendix A should be used. There should also be some discussion of how certification of compliance within this framework could be achieved. Additionally, the document should anticipate next steps to be taken by DHS that include special designation of critical infrastructures and nodes, as well as sector specific implementions of the framework which could be mandatory.

Type: E - Editorial, G - General T - Technical

2	IDA	Graeme Douglas	G				The framework functions all relate to each other and need to be considered in an integrated and iterative fashion. The framework considers this only indirectly by including an "adaptive" tier in the maturity model. It is essential that organizations consider cybersecurity a dynamic, requiring continuous re-evaluation and assessment. The iterative element of cybersecurity is an important foundational element of successful cybersecurity that should be considered in the framework core.	Include a graphic and explanatory text illustrating the iterative nature of the cybersecurity functions. The "Plan-Do-Check-Act" + repeat cycle is an example.
3	IDA	Graeme Douglas	G				The draft framework does not have any inherent mechanism for guiding the customization of implementations by considering the specific threats faced by a particular, sector, sub-sector or organization. For cybersecurity to be most effective they should be informed by the specific threats facing the organization.	Update the target profile definition process that includes a "threat model" for each infrastructure to address vectors, actors, and timelines.
4	IDA		G	7	282	2.2	The discussion of the Framework Profile provides insufficient guidance for small and medium-size businesses to implement efficiently.	See comment on Section 2.4 below. By describing a "Tier 0" it allows more basic guidance for small to medium-size businesses who may lack a functional cyber security program.
5	IDA	Graeme Douglas	G	9	332	2.4	The implementation tiers in the maturity section should have a zero base but the zero of the scale should be reserved for organizations to identify areas where they have no activity, not for credit partial implementation as the draft proposes. The framework implies some partial level of activity even when there is none. This is simply inaccurate and will complicate future analysis difficult.	Provide a zero level to allow a no-activity or extremely limited activity to be more accurately described.

6	IDA	Graeme Douglas	G	11	390	3.0	The framework document provides a section that describes, at a very high level, how an organization would get started with the implementation of the framework. This is insufficient to guide most organizations. The needs of an organization currently doing nothing, an organization with a flawed but existing program, and an organization with an excellent cybersecurity program are fundamentally different.	Provide an implementation appendix that describes an implementation scenario for each infrastructure and type of organization described above. Provide a robust write up of the process of mapping existing controls into the framework and closing any gaps identified at that time.
7	IDA	Graeme Douglas	G	3	159	1.2	The framework, as written, focuses heavily on risk management. This aspect of cybersecurity is already well covered by a number of existing standards, including NIST SP 800-53, many of which are documented in Appendix A. Other important aspects of cybersecurity are not given much attention in the framework. A key shortcoming of the cybersecurity discipline is the inability to place the discipline in the larger context of an organization and to articulate the value of cybersecurity to business leadership. Cybersecurity decisions should be an integral part of the days to day business decisions made in an organization rather than made in isolation. Cyber risk should be considered as an integrated component of business risk.	The framework should recommend that cybersecurity be managed as an element of an organization's risk portfolio and should be integrated into the larger body of business processes and the decision-making processes for the organization. This recommendation is tightly coupled to the following recommendation related to governance.

8	IDA	Graeme Douglas	G	3	159	1.2	The draft framework has minimal discussion of the governance needs of cybersecurity. Cybersecurity considerations are pervasive in organizations that rely heavily on information technology in the execution of their day-to-day business. The implication of this is that successful cybersecurity must meet the potentially conflicting needs of multiple stakeholders. The governance of cybersecurity must therefore be constructed in such a way that cybersecurity needs can be balanced against the other business needs the organization.	Add a section that provides a comprehensive discussion of organizational structures that empower consideration of cyber security risk along with other risk factors. Provide examples of cybersecurity governance structures such as roles and functions of a Chief Risk Officer, reporting structures for a CRO, and Board level governance.