Comments template for Preliminary Cybersecurity Framework

Submitted by: Information Assurance Advisory, LLC
Date: Dec. 13, 2013

Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
IAAdvisory	Roger Callahan	G	All	All	All	The Cybersecurity Framework (CSF) can provide a necessary common language and mechanism to foster an organization's communications related to cybersecurity risks and to assist them in examining the organization's current state of cybersecurity risk management. Recognizing that this effort on the Framework 1) has already created broad participation across various stakeholder communities, 2) is understood to be a preliminary and living document that must evolve over time with changes in technology, the knowledge of new threats and new effective controls and counter measures, and 3) will require an assignment of responsibility and support to continue the roles and efforts demonstrated in this preliminary effort, we offer a suggested change to address the later item.	Be more specific in the body of the framework document, not just an Appendix comment, on the responsibilities and process to be used to evolve the document overtime. This stated commitment will be important, as many efforts have come and gone that have tried to coalesce the information technology and communication communities. By stating a commitment to continue the collaboration efforts demonstrated during the preliminary framework development and identifying the structure to support such an effort, which is support by both executive and congressional leadership, can increased the confidence of a likely broader application going forward. A supported and focused level of broad collaboration is essential to success in the area of cybersecurity. The Framework process and effort is an opportunity for this sustained collaboration; if it is effectively managed and adequately resourced.

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

IAAdvisory	Roger Callahan	G	All	All	All	The requirement to identify the level of "resiliency" for organizational functions, process, operations, systems, and applications is not mentioned as a component of the risk management assessment. This is most important requirement, especially applicable for those providing critical infrastructure services and should be stated as an objetive.	An organizations ability to continue operations in the cyber domain is directly tied to their "Resiliency" decisions and approaches taken to mitigate business and environment risks. For critical environments, this resiliency is highly influenced by the information technology architecture being employed. Suggest, the Framework include some elaboration on this requirement; as resiliency considerations cuts across and influences the Identify, Protect, Detect, Respond and Recover Core Functions and the decisions used to manage cybersecurity risks.

IAAdvisory	Roger Callahan	G/E	3 and 15	173 and 466	1.1 and Appendix A	The document is assuming an organization has some formally assigned and developed responsibilities for risk management. In previous comments provide during the process of developing the Framework, the topic of 'organizational governance' was identified as an important element to be addressed in order to have a compressive risk management and information technology governance structure implemented with mature organizational management processes. The complexity of cybersecurity risk management today requires strong governance within an organizations in order to have some chance of managing the risk. Not emphasizing this necessity will diminish the effectiveness that can be achieved through use of the Framework.	Change: "The Board of Directors for corporations or the head Corporate Executive, as appropriate, must establish formal responsibilities within the organization for accomplishing cybersecurity risk management for the organization to effectively utilize this framework. Ideally this assignment should be within the organization addressing other operational risk management efforts within the organization. With this assignment of responsibility, the Framework gives organizations the ability to dynamically select and direct improvements in both IT and ICS cybersecurity risk management." Change: The Governance Category within the Identify Function of the Framework should be listed first. Without appropriate governance, the ability to managed cybersecurity risks in any enterprise of significant size is doomed.

IAAdvisory	Roger Callahan	G/E	8	307, 466 and 501	2.3 and ID.RA-2 and RA.3 and Appendix C	As noted in NIST 800-53 , organizational assessments of risk, must use specific and credible threat information. Realistic assessment of risk requires an understanding of threats to and vulnerabilities within organizations and the likelihood and potential adverse impacts of successful exploitations of vulnerabilities by those threats. Threats can be both malicious and unintential and must cover the full spectrum of hazards that need to be assessed. It is essential that organizations have well defined basis and factual information for the threat and hazard landscapes to be addressed. Gaining authentic information from appropriate threat identification components and organization is not well organized to assist in assessments. Assessments done without full knowledge of threats and hazards can produce ineffective controls and countermeasures.	More directly highlight and expand guidance on theimport need for risk assessment organizations/process to formally develop threat and hazard models (based on authoritative sources) which address business and operational environmen. Also, this is a continuing requirement necessary to assure new threats and hazards are incorporated and reflected in the risk assessments. Limited knowledge of threats and hazards and their likelihoods on the part of assessors can invalid all subsequent protection, detection, response and recovery plans. Add to Appendix C "Threat and All Hazard Models" as this is a area for definite improvement
IAAdvisory	Roger Callahan	T	21	466	PR Section	The value of enterprise architecture efforts to the efforts to assure consistent and appropriate protective methodologies is not articulated at all with the Framework and reflects a significant gap in the Framework. Suggest in either the discussion of Protection Function or in the Core Framework itself there be a category on Enterprise Architecture.	Include a PR.EA-1: Identify or establish an Enterprise Architecture (EA) to evaluate the protection consistency and approaches across the organizations information systems and communications environment based on the risk assessment requirements and technology employed. Useful Information references can include The Open Group Architectural Framework (TOGAF) and "Common Approach to Federal Enterprise Architecture"

IAAdvisory	Roger Callahan	G	28	485	Appendix B	During a breakout session on Privacy and Civil Liberties at the 5th Workshop, Harriet Pearson, peovided a "Strawperson Discussion Document" dated Nov. 14, 2013 on Privacy methodology. We support the general principles and considerations presented to guide the scope and content of the privacy methodology and strongly support that protecting civil liberties pertains overwhelminlgy to govermental organizations. The protection of PII should be reflected as another of the several types of information to be protected within an organization's cybersecruity program.	Suggest the methodolgy of Appendix B at this stage of the Framework's development be a more general articulation of privacy considerations related to cybersecurity activities (similar to Ms. Pearson's strawperson document) versus trying to match the Function and Categories structure of the Core Framework. Methodology and informative references should be consistent with those identified in the Core for managing the risks of other types of sensitive organizational information. Useful privavcy specific informative references can be reflected but legal and regulatory requirements and organizational policies will directly effect the risk management, controls and countermeasures efforts organizations employ.