To Whom It May Concern -

In response to this RFI, rather than suggest specific content, I would like to bring NIST's attention to several conceptual perspectives that I believe have so far been underrepresented in the discussion so far.

Perspective 1: ***A Need for Common Conceptual Framing***

First, I believe the potential value of a successful framework will not be in the content, but in the conceptual model the content is organized around. One of the primary problems facing us as individual organizations and as a nation is the not only the lack of a common cyber security lexicon, but also significantly incomplete and often incompatible views as to what comprises cyber security itself. This point can be illustrated in three ways:

1. After attending the recent NIST Framework Workshop, it was evident that many speakers were discussing only component pieces of cyber security (e.g., information sharing), and not the entirety of the problem (e.g., procurement). The result was a grab-bag of security ideas that could not be evaluated in terms of each other or their role in security as compared to the rest of the ideas shared. The discussion lacked the structural and conceptual rails required to guide the participants down the path of solving the same problem. I was left wondering "How does this all fit together?".

2. One of the critical infrastructure sectors recently asked their pertinent government agencies (there were 4 represented) for guidance on which federal tools and frameworks should be used, by whom, when, and why. Industry believed the tools lacked appropriate descriptions. After investigation, the fundamental issue was not that the tools lacked descriptions, but that those using them were not aware of the full scope of problems which needed solving. Participants lacked a common, complete conceptual framework in which to evaluate the tools. This lack of a broad, structured, conceptual model made it difficult for them to assess or use other content.

These are only two examples of many. This is a problem that occurs in almost every cyber security dialogue – even among cyber security SME's. For this reason I believe that one of

the primary values of the NIST Framework should be in providing that common view - not only of security practices, but also how those practices fit together to reduce risk. One might call it a "cyber security algorithm" where program, practice, and control domains are variables which must be used to solve for "assured risk reduction". In such a model, individual best practices and content elements can be tied to each “variable” and can be selected by industry. This provides some assurance that they are all working coherently together.

Such a model could conceivably be broken down into six different layers of activities (*national, sector, business, architecture, implementation, operation*) broken into two dependent but different risk life cycles: Strategic (*risks from cyber systems*) and Operational (*risks to cyber systems*).

In this manner, the structure of the NIST framework could be used independently of the content to educate readers, assist them with communication, and be helpful as a tool to solve for specific cyber security outcomes.

Perspective 2: *Non-Cyber Business Maturation and Foundations*

In my experience, many organizations would have very successful cyber security practices, but their extra-cyber practices are not able to effectively use or support the good cyber-specific ones. These extra-cyber practices include procurement, marketing, scheduling, business operations, development, testing, sales, database administration, communications, etc. It is often said that "good security isn't bolted on, it's baked in". That is only partially correct. Good security is good business - there is often little to distinguish the two. Security usually fails long before anyone with "information security" in a title or department name is involved. As such, I believe the NIST framework should focus more on identifying good **business** practices which lead to successful cyber security than on **cyber-specific** ones. It should also keep in mind that those most in need of the framework are the least likely to understand their own role in the cyber security problem domain.

Perspective 3: *Quality Assurance & Human-Centric Cyber Security*

As we have seen many times now - in the cases of some large and well known security breaches of organizations who were **fully aware and invested in** cyber security best

practices - the problem we are facing is not just one of knowledge, but one of consistency of practice. It is relatively difficult, the way we do business today, to assure the application of best practice (whether through internal business incentive or government regulation) in a consistent manner. The NIST framework should attempt to improve this consistency.

One aid in achieving that consistency is identifying where cyber security faults - which are really just errors made by a human in an authorized role somewhere on a timeline - are occurring and describing them in terms of human-role/authorized-action control pairs. Examples could include: *CEO/SuccessDefinition, Vendor/FeatureInclusion, Vendor/QualityAudit, ProcurementOfficer/ProductEval, Subcontractor/OrganizationBridging, ITManager/WorkPrioritization, etc.* Putting these pairs into a timeline or lifecycle model would allow us to describe desired cyber security state and control points in a manner that would: Be valid through most possible iterations of technology, allow users of the framework to better identify which best practices were applicable when and to whom, reduce cost by placing controls as close to the fault source as possible, and help increase consistency by more effective and efficient control placement.

In closing, I believe that the NIST cyber security framework has the potential to be an extremely valuable tool, but that its success will depend on its framing and structure. It must speak to non-traditional cyber-security audiences in their own voices and simplify otherwise high levels of detail in a way that enabled significantly better dialogue than we as a community have been able to achieve so far.

Thank you for your time and efforts.

V/R,

Jack Whitsitt/Energysec