Comments o NIST Preliminary Cybersecurity Framework

e-Management is a small business that provides IT and cybersecurity services and software to organizations in one or more critical infrastructure (CI) sectors. We appreciate the opportunity to provide our input and feedback to NIST o the Framework and hope that our suggestions may be useful in helping the Framework become easier for other small business CI owners or operators or those providing products and services to CI sectors to adopt.

Our comments address the questions requested by NIST for reviewers to consider.

1. Does the Preliminary Framework:
    a. Adequately define outcomes that strengthen cybersecurity and support business objectives?

        Comment: The document does include several references to outcomes for the Framework Core and Current and Target Profiles. For example, lines 245-247 describe categories of outcomes associated with the Identify Function of the Framework Core such as Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy. However it is unclear what specific outcomes are desired in each of those categories. Lines 399-400 state that "Organizations should have at least basic capabilities implemented in each of these areas, and can begin to review what particular categories and subcategories they currently use to help achieve those outcomes." It would be helpful, especially for small businesses, if NIST could provide some examples of what it considers "basic capabilities" that organizations should implement in each of these outcome categories.

    b. Enable cost-effective implementation?

        Comment: It depends. To-date we've tested the Framework using two different approaches to create a current and target profile. One approach took less than a day to complete. The second approach which was more substantive and comprehensive took weeks. The two approaches produced different results. While the one day approach would have been considered "cost-effective", it produced high-level results which, when compared to the results of the second more comprehensive approach, did not provide as much insight into some areas as the comprehensive approach did. In addition, the Framework document offers n information or guidance o what a reasonable timeframe might be to implement the Framework (e.g. 12 months, 2 years, etc.). This would impact costs. We believe the full costs for implementation of the Framework should also take into account the costs for prioritizing or implementing specific actions resulting from the risk assessment and gap analysis. This could quickly become cost prohibitive for lot of small businesses.

e-Management recommends that some organizing body (e.g. NIST, DHS, industry groups, etc.) convene a voluntery group of similar size organizations who would implement the Framework in the same way in order to be able to have an apples to apples comparison of time, costs, and resulting outcomes from the implementation of the Framework.

c. Appropriately integrate cybersecurity risk into business risk?

Comment: Yes. We believe NIST did a good job of appropriately integrating cybersecurity risk into business risk in the Framework. Some examples include the inclusion of the Business Environment, Governance, and Risk Management Strategy categories in the Identify function.

d. Provide the tools for senior executives and boards of directors to understand risks and mitigations at the approprate level of detail?

Comment: The Framework document itself does not speak much to these two audiences. Several collateral pieces that have been developed outside of the Framework are helpful (e.g. the executive overview for senior executives). e-Management recommends the inclusion of a section in the Framework document that addresses senior executives. Alternatively, NIST could include the aforementioned exective overview document as an Appendix to the Framework.

e. Provide sufficient guidance and resources to aid businesses of all sizes while maintaining flexibility.

Comment: Perhaps NIST might consider including as an Appendix to the Framework a listing of the various sector coordinating council websites as resource for assistance. e-Management found the workshops hosted by NIST to be especially helpful in understanding the context of the Framework. We recommend that during the first 12 months following release of the v1.0 of the Framework in February 2014, that NIST and DHS consider hosting "orientation workshops" in person, virtually or a combination of both to help organizations better understand how to implement the Framework.

f. Providing the right level of specificity and guidance for mitigating the impact of cybersecurity measures on privacy and civil liberties.

Comment: e-Management appreciates the emphasis on privacy and civil liberties in the Framework and offers no additional comments.

g. Express existing practices in manner that allows for effective use

Comment: For the most part. The informative references are very useful.

2. Will the Preliminary Framework, as presented:
    a. Be inclusive of, and not disruptive to, effective cybersecurity practices in use today, including widely-used voluntary consensus standards that are not yet final?

       Comment: The Framework does a good job of identifying and including informative references to effective cyber security practices in use today, including voluntary consensus standards that may not yet be final.

    b. Enable organizations to incorporate threat information?

       Comment: The Framework document is largely silent o this topic. Lines 326-327 state that "The Tier selection process considers an organization's current risk management practices, threat environment..." In Section 3.2, there is mention of incorporating "emergent risks and outside threat data" as part of conduting a risk assessment. However, very little is said about how an organization could or should accomplish that.

3. Is the Preliminary Framework:
    a. Presented at the right level of specifity?

       Comment: In general the document does a good job of describing <u>what</u> needs to be done. It is less clear on <u>how</u> various outcomes can be achieved (see previous comments).

    b. Sufficiently clear on how the privacy and civil liberties methodology is integrated with the Framework Core?

       Comment: e-Management recommends that Appendix B be incorporated in the Framework Core as categories (outcomes) and subcategories rather than as a separate Appendix.