From: Bodre, Laura [USA]
Sent: Tuesday, January 10, 2017 4:30 PM
To: Barrett, Matthew P. (Fed)
Cc: McKinney, Reggie; Jackson, Helen; Etherton, Anna; Cleghorn, DeShelle; Blight, Garrettson [USA]; Rian, John A. [USA]; Kellenbarger, Christopher [USA]; Bucher, Timothy [USA]; Singh, Kesh [USA]
Subject: C3VP feedback on Framework v1.1

Hi Matt,

Thank you for providing the C3 Voluntary Program team with the opportunity to preview Framework v1.1. I've attached our feedback here. Please let me know if anything needs clarifying.

Thanks again, and have a great evening!
Laura

Laura Britton Bodré
Booz|Allen|Hamilton

[Attachment Copied Below]

Cybersecurity Framework Version 1.1
Critical Infrastructure Cyber Community (C_3) Voluntary Program Feedback

In response to the release of Cybersecurity Framework Version 1.1 by the National Institute of Standards and Technology on January 10, 2017, the C_3 Voluntary Program submits the following feedback:

- Recognition of the process since the inception in the note to reviewers and the questions are good, but we would add 1) What are the metrics or measurements that the corporation/agency currently uses to track performance of the Framework, and 2) What are the tools/techniques you employ to address aspects of the 'core' Framework?
    - Consolidating industry feedback in this regard would assist the C_3 Voluntary Program to recommend various effective implementations. Since this will not be a question in the data call, perhaps each of these can be a breakout session at the workshop; our concern is giving the organization enough time to consolidate detailed responses.
- We respect the changes that they tried to make to the tiers, but we expect that industry will still not understand how to use them and what the relationship is with the profiles. Our only recommendation here would be to add an appendix with a sample profile and describe the relationship in the tier for the example use case.
    - Users have a desire to see/know what "correct use" looks like, whether through examples, templates, published use cases, etc.
- Figure 1: We think the Framework will be better branded if there is an image or logo that represents the Framework. This has not effectively occurred since the beginning. Perhaps this is another area that the C_3 Voluntary Program can help with from a graphic artist perspective to put some options in front of NIST before the final release. An icon will help 'sell' and get brand recognition for implementation.
- There is a mention of Information Sharing and Analysis Centers (ISACs) in the text, but not a mention of the role of the Department of Homeland Security (DHS). It would be good for DHS if there was a recognition of the DHS role somewhere within the document. If there are other agencies that NIST also wants to recognize, we would recommend an appendix here as well.
- Other NIST publications: Somewhere in the document (perhaps an appendix again) there should be a listing of relevant informative references beyond the security controls. For instance, the NIST Special Publication (SP) 800-150 for *Threat Information Sharing*, SP 800-160 *System Security Engineering*, SP 800-161 *Supply Chain Risk Management*. It is good that they list the 800-82, but it seems incomplete with the changes they have made if they don't list the others somewhere.
- Early in the document they use 'ICS' and later they use 'OT' without spelling out the acronym of Operational Technology. There needs to be consistency and/or a description of relevant differences.
- The section on privacy seems forced and disjointed in the context of the rest of the document; it may be better to just recognize the importance of privacy and civil liberties and point to the NIST Internal/Interagency Report (NISTIR) 8062 – *An Introduction to Privacy Engineering and Risk Management in Federal Systems.*

- We like the addition of the Federal Alignment section, but it is short. We hope they specifically look for feedback from Federal entities to further capture what else may be relevant. We suspect that the larger question will still remain regarding how to use the Framework and still answer the mail on any Risk Management Framework (RMF) requirements (or else the U.S. Government will continue to just do Federal Information Security Management Act (FISMA)/RMF as stated in the Office of Management and Budge (OMB) memos and the RMF series without really regarding the Framework in any way – which may be fine, but the Government needs to get that message before they default to that approach.
- As we mentioned to Matt Barrett on section 4 for measurements and metrics, we think the current approach misses the mark. There should be a detailed exemplar of potential metrics and measurements for the Framework in an appendix so that organizations have a starting point for implementation and can select what works for their environment. Without this, it will be difficult to ever get traction beyond a high level.
- The adjustments to the Core are fine. It would be beneficial for the C_3 Voluntary Program or NIST to provide an endorsed list of open source or government resources for any subcategory to lower the barrier to entry. However, we realize that even if it is a government resource, neither organization would likely 'endorse' anything since effectiveness relies on individual implementation regardless of the tool or technique.
- The Framework is touted as being adaptable and flexible; however, many users at the lower State and local levels as well as smaller organizations who have expressed great interest in using the Framework have stated that they have a difficult time knowing how to appropriately scale down from an enterprise level to something more appropriate for their organization's size.