From: **Geyer, Michelle L.**
Date: Wed, Apr 19, 2017 at 12:24 PM
Subject: Department of Veterans Affairs - Comments for National Institute of Standards and Technology (NIST) Cybersecurity Framework Release, Version 1.1
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

To Whom it May Concern:

Please accept attached comments from Department of Veterans Affairs for consideration for National Institute of Standards and Technology (NIST) Cybersecurity Framework Release, Version 1.1.

Thank you,
Michelle

Michelle L. Geyer
IT Specialist
Office of Information Security
Cyber Security Policy and Compliance (005R2)

Department of Veterans Affairs
1100 First St, NE - Cubicle 410B
Washington DC 20002

COMMENT MATRIX FOR NIST FRAMEWORK V1.1

#	Section	Recommendation / Comment	Comment From	Disposition / Action	Date	Status
1.	1.0 – lines 180-184	Framework Introduction	EPMO	Consider adding assistance and/or references for entities that straddle multiple countries to help move toward goals of common language and international cooperation.	3/23/17	
2.	2.0 – lines 263-265	Framework Basics	EPMO	Please, clarify last segment "including creation of common Profiles." Considering the guidance in section 2.3 (lines 452 – 458), it is unclear to which "common Profiles" refers. Is it meant to be common across an enterprise, or common across multiple entities? This seems contradictory. Perhaps an example of a common profile crossing different entity types would be helpful, if that is what is intended	3/23/17	
3.	2.2 – line 330	Framework Implementation Tiers	EPMO	These tiers are useful & while currently voluntary, is the goal to institute these as industry standard requirements as the adoption rate for the standard rises? If so, will implementation be tied to SP 800-53 controls as well as these subcategories? Is there a plan to create a crosswalk between SP 800-53 controls and these subcategories?	3/23/17	
4.	2.2 – line 330	Framework Implementation Tiers	G.L. Coulbourn	The added explanation of the relationship between Implementation Tiers and Profiles was rather brief/ vague. Suggest providing a more thorough explanation of how the Tier selection affects Framework Profiles.	2/28/17	
5.	3.3 – line 585	Including the SCRM section to v1.1 is beneficial in that it helps organizations make informed buying decisions about cybersecurity products and services. When given a pre-decided list of cybersecurity requirements,	G.L. Coulbourn	N/A	2/28/17	

#	Section	Recommendation / Comment	Comment From	Disposition / Action	Date	Status
		organizations are better informed on which products/services will address cybersecurity gaps and/or achieve their desired cybersecurity outcomes (Target Profile).				
6.	3.6 – line 660	**This comment is for VA Consideration ONLY**	EPMO	Consider having Legal take a look at this section to determine if a caveat is a good idea when referencing this document as a VA standard to avoid potential conflicts with existing legal standards.	3/23/17	
7.	4.0 – line 745	Measuring and Demonstrating Cybersecurity	J. Raia	Who would be categorized as a 'dependent'? Consider defining in glossary (glossary includes other terms such as buyer, supplier, etc.)	2/28/2017	
8.	4.1 – line 796	Correlation to Business Results	EPMO	Consider adding something along the lines of "It's hard to measure the absence of a negative," to further illuminate this As so many of us in cybersecurity are familiar with the idea that when nothing is happening it may seem to outsiders that we aren't producing results, when in truth we work hard to make sure "nothing happens."	3/23/17	
9.	4.1 – line 801	Correlation to Business Results	J. Raia	Should 'enabling cybersecurity' be 'ensuring cybersecurity'?	2/28/2017	
10.	4.2 - Table 1 – lines 811-849	Types of Cybersecurity Measurement	EPMO	This table & section are a bit unclear. Yes, the terms "metrics" and "measures" are defined in lines 746 – 753. "Metrics" adheres to standard usage & seems more intuitive, but consider re-naming "measures" to be "control measures." That seems to be a natural transition for SP 800-53 usage and so will feel more intuitive to those (many!) users. It may also help ease adoption.	3/23/17	

COMMENT MATRIX FOR NIST FRAMEWORK V1.1

#	Section	Recommendation / Comment	Comment From	Disposition / Action	Date	Status
11.	Table 3 – page 32	Access Control Category (PR.AC)	J. Raia	Function: Protect (PR), Category: Identity Management, Authentication and Access Control (PR.AC): '…unauthorized access to authorized activities and transactions'—Clarification?	2/28/2017	
12.	Table 3 – page 32	Access Control Category (PR.AC)	G.L. Coulbourn	To stay consistent with the CIA Triad, I agree with the decision to include authentication and authorization under the Access Control Category, and create a subcategory that accounts for identity proofing	2/28/17	
13.	End of Appendix A	Page 45, Line 897- Center for Internet Security (CIS) Critical Security Controls for Effective Cyber Defense (CSC) link takes user to the Center for Internet Security homepage; should there be a more direct link to the controls list?	J. Raia		2/28/2017	
14.	End of Appendix A	Page 46, Line 911- NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4 reference should state '(including updates as of January 22, 2015)' instead of January 15, 2014	J. Raia		2/28/2017	