From: **doe.ocio.executive-secretariat**
Date: Fri, Apr 7, 2017 at 1:05 PM
Subject: DOE's Response to ECPC Requested - Review of NIST Cybersecurity Framework
To: "cyberframework@nist.gov" <cyberframework@nist.gov>
Cc: Nolan, Matthew, Green, Robbie, Peace, Cheryl, Long, Bryan

National Institute of Standards and Technology:

In response to your request for review and comments on the proposed updates to the original National Institute of Standards and Technology (NIST) Cybersecurity Framework v1.1, The Department of Energy (DOE) concurs with the NIST Cybersecurity Framework and provides the attached comments for consideration to improve consistency and clarity of the draft document.

Thank you for providing us with the opportunity to review.

R/S

OCIO Executive Secretariat

==========
The National Institute of Standards and Technology (NIST) has been working to update the original NIST Cybersecurity Framework that was first released in 2014. The update was released on January 10th and contains many of the anticipated revisions (from the RFI and workshop) as well as:

- Significant updates to the cyber supply chain risk management
- Defined cybersecurity terminology
- Identity Management and Access Control updates (including "identity proofing")
- A new section on cybersecurity measurement

Comments on the proposed updates are due by April 10, 2017.

The draft version can be located here: https://www.nist.gov/cyberframework/draft-version-11 To submit comments and questions to NIST, please contact them at this email address.
mailto:cyberframework@nist.gov

[Attachment Copied Below]

Comment #1

- Page #: iii
- Line #: 34
- Section: Notes to Reviewer
- Comment Type: Administrative
- Comment: Per the question in the NIST document – Is there a better label than "version 1.1" for this update?
- Suggestion: If the changes are significant, then suggest moving changes from Version 1.1 to Version 2.0
- Rationale: In subsequent releases of documents, the major number is increased when there are significant jumps in functionality
- Organization: Department of Energy
- POC: OCIO

Comment #2

- Page #: 6
- Line #: 102-107
- Section: Executive Summary
- Comment Type: Substantive
- Comment: Recommend deleting this paragraph
- Suggestion: N/A
- Rationale: The restrictive message of this paragraph seems to be unnecessary and potentially at odds with the expansive message of the paragraph that precedes it (Lines 94-101)
- Organization: Department of Energy
- POC: OCIO

Comment #3

- Page #: 6
- Line #: 109-110
- Section: Notes to Reviewer
- Comment Type: Substantive
- Comment: Possible missing word in sentence: "NIST will continue coordinating industry as directed in …".
- Suggestion: "NIST will continue coordinating **with** industry as directed in …".
- Rationale: Softens the meaning to the intended level.
- Organization: Department of Energy
- POC: OCIO

Comment #4

- Page #: 18
- Line #: 488
- Section: 3.0 How to Use the Framework
- Comment Type: Substantive
- Comment: This section could benefit from an example or use-case to walk the reader through exactly how the Framework might be used in a typical, practical situation.
- Suggestion: N/A
- Rationale: The section describes how the Framework CAN be used, but not what it would look like to actually use it. The description is perhaps too abstract for practitioners to easily adopt and use the Framework.
- Organization: Department of Energy
- POC: OCIO

Comment #5

- Page #: 20
- Line #: 740
- Section: 3.7 Federal Alignment
- Comment Type: Substantive
- Comment: 11 OMB Memorandum M-16-03, FY 2015-16 Guidance on Federal Information Security and Privacy Management Requirements, http://dpcld.defense.gov/Portals/49/Documents/Privacy/Memorandum/OMBMemorandumM-16-03.pdf
- Suggestion: If appropriate, replace with reference to current OMB Memo M-17-05, Fiscal Year 2016 - 2017 Guidance On Federal Information Security And Privacy Management Requirements (Nov 4, 2016) (12 pages, 13.8 mb).
- Rationale: Newer OMB Memo was released
- Organization: Department of Energy
- POC: OCIO