From: **Aaron P. Padilla**
Date: Mon, Apr 10, 2017 at 3:16 PM
Subject: API Response to the Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

Dear Mr. Games:

The American Petroleum Institute (API) welcomes the opportunity to respond to the Request for Comments to the Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity.

Please see our submission attached.

With kind regards,

Aaron

Aaron Padilla, PhD
Senior Advisor, International Policy | API | 1220 L. Street, NW, Washington, DC 20005 USA

[Attachment Copied Below]

Submitted via cyberframework@nist.gov

10 April 2017

Edwin Games
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Subject: **API Response to the Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity**

Dear Mr. Games:

The American Petroleum Institute (API) welcomes the opportunity to comment upon the Request for Comments to the Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity (hereafter referred to as the "Cybersecurity Framework" or "CSF." API is the only national trade association that represents all aspects of America's oil and natural gas industry. Our more than 625 corporate members, from the largest major oil company to the smallest of independents, come from all segments of the industry. They are producers, refiners, suppliers, marketers, pipeline operators and marine transporters, as well as service and supply companies that support all segments of the industry.

Cybersecurity is a priority for the oil and natural gas industry. Most, if not all of the largest API member companies manage cybersecurity as an enterprise risk with oversight from Boards of Directors and Senior Executives. As operators of and service providers to energy critical infrastructure in the United States and globally, protecting networks from cyber-attacks is a priority of API's members. Please see below for overarching comments, followed by answers to the questions in CSF Draft Version 1.1, followed by an attached detailed response.

- **API member companies continue to support the Cybersecurity Framework (CSF), including V1.1, as the pre-eminent standard for companies' cybersecurity programs and for policy making globally.** We support the CSF because it is (a) comprehensive, (b) a risk management approach, (c) scalable to different types and sizes of companies, and (d) widely used across industry.

- **API encourages NIST to continue global outreach programs to help align cybersecurity regulations or requirements across the world to the CSF.** The common taxonomy and method of the CSF benefits multi-national API members who can use common processes to address cybersecurity issues rather than having to devote scarce resources to managing different nuances of different regimes across the world.

- **API supports the inclusion of Supply Chain in the CSF, but we strongly urge NIST not to incorporate Supply Chain as its own new Category.** Supply Chain is a valid lens (context) through which to look for risk, but such cybersecurity risks should be woven into the Framework. For example, Cloud Computing, Internet of Things, and Mobility are also valid lenses or contexts, but these are not separate categories in the CSF. Adding all of these additional cybersecurity risks as separate Categories would greatly expand the CSF; a better solution would be to add Supply Chain to specific items within sub-categories under the relevant existing category (e.g., Asset Management, Risk Assessment)

Overall, API continues to support the use of the Cybersecurity Framework (CSF) and believes that NIST is a prime example of how government can work cooperatively with industry to manage risks, with the goal of providing reliable and affordable energy to the nation. Specifically, API supports the use of voluntary guidance over regulation in managing cybersecurity as it allows industry critical flexibility in managing threats in a dynamic and ever changing environment.

API's answers to the questions posted in the CSF V1.1 draft are as follows:

1. **Are there any topics not addressed in the draft Framework Version 1.1 that could be addressed in the final?**
   - **Threat Intelligence.** We believe "(using) threat intelligence" is sufficiently mature to be included as its own category within Detect.
   - **Implementation Tiers.** We believe Implementation Tiers need more work. Tiers are selected for the organization as a whole which ostensibly guides the creation of profiles but an organization may not aspire to have each and every control meet the same maturity level. For example, some controls, perhaps around critical infrastructure or data, will need to exceed the organizational tier. A company's tier selection may give a general idea of philosophy but would or could mask actual control implementation (which is likely of more importance if someone is assessing a potential partner.)
   - **New subcategories.** We recommend that for the new subcategories on documentation, removal/disabling of unnecessary applications/services that NIST include text that states that awareness/education is sprinkled through the document and consequently identifies the importance of this item.
   - **Definition of External/Third Parties.** We recommend that CSF V1.1 should include this definition for External/Third Parties: "external organizations including vendors, contractors, cloud providers and other service providers where access is based upon a restricted trust model."
   - **Privacy/Civil Liberties.** We recommend that the privacy / civil liberties section should be updated to include text covering working with third parties.

     Please note that details on the above may be found in the attachment.

2. **How do the changes made in the draft Version 1.1 impact the cybersecurity ecosystem?**
   - We believe that the changes are an improvement. The updates for Supply Chain provide a good framework for managing this difficult problem (provided these are distributed through the existing document rather than kept in a Supply Chain category). The addition of authentication and identity proofing to the previously named Access Control category brings this section more in line with the Identity and Access Management programs, which most companies have. The measurement text is a good first step in helping to define metrics and measures although additional treatment, either within the framework proper or perhaps better in a guidance document would help step an organization through the process.

3. **For those using Version 1.0, would the proposed changes impact your current use of the Framework? If so, how?**
   - The proposed changes would not impact API member companies' current use of the CSF. We expect that API members would incorporate the core changes into what is already being done.

4. **For those not currently using Version 1.0, does the draft Version 1.1 affect your decision to use the Framework? If so, how?**
   - The changes are mostly incremental and consequently are not "game changers," so we doubt they would drive a company not using CSF 1.0 to use it.

5. **Does this proposed update adequately reflect advances made in the Roadmap areas?**
   - Yes, although we believe "Automated Indicator Sharing" and "Data Analytics" are mature enough to be included in the framework core as a sub-category to a new Threat Intelligence category within Detect.

6. **Is there a better label than "version 1.1" for this update?**
   - We believe that "Version1.1" is sufficient.

7. **Based on this update, activities in Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap? Are there any areas that should be removed from the Roadmap?**

   - **Continuous improvement to update Informative References and relevant Categories and Subcategories.** API encourages NIST to continue to revise the Cybersecurity Framework Core with updated Informative References and relevant categories and subcategories. One example would be including a new category of "Using Threat Intelligence" under the "Detect" function; sub-categories would include "Automated Indicator Sharing" and "Data Analytics". As virtually all critical infrastructure sectors have at least one Information Sharing and Analysis Center (ISAC) and with the growing acceptance of the STIX/TAXII information sharing specifications, API feels this category is sufficiently defined to be included in the framework core.
   - **Supply Chain.** API applauds the additional of Supply Chain considerations within the CSF. While we believe the sub-categories are correct, we disagree with the inclusion of these within a Supply Chain category within Identify. There are a couple of issues with the current implementation. Some elements clearly do not belong in Identify. "ID.SC-5 Response and recovery planning and testing are conducted with critical suppliers/providers" is a clear example. Response and recovery planning are categories under "Respond" (RS.RP) and "Recover" (RC.RP) so including such planning in Identify makes no sense. Likewise, "ID.SC-4: Suppliers and partners are monitored to confirm that they have satisfied their obligations as required. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted" would seem to fit under "Detect: Security Continuous Monitoring (DE.CM); there is already a subcategory (DE.CM-6) covering "External Service Providers" which are at least a subset of supply chain.

“Supply Chain” is a valid lens (context) in which to look for risk but should not be a category. For example, Cloud Computing, Internet of Things, and Mobility are also valid lenses or contexts, but these are not separate categories in the CSF. Adding them as such would greatly expand the CSF needlessly. In virtually all of these cases, the elements already in the CSF apply; one needs to “inventory” supply chain entities, one needs to do a risk assessment, etc. One can add supply chain specific items as sub-categories but one should do so under the existing category (like Asset Management, Risk Assessment, etc.) but not as a separate category.

- **Recommendations for adding and removing other specific items.** Items added to the draft, ***Authentication***, ***Federal Agency Cybersecurity Alignment***, and ***Supply Train*** can be removed. If our recommendation regarding the ***Threat Intelligence*** category is accepted, then ***Automated Indicator Sharing*** and ***Data Analytics*** can likewise be removed. Additional work is needed on ***Conformity Assessment***. The ***Cybersecurity Workforce*** item is not specific to the framework; NIST should continue to work this issue via efforts like National Initiative for Cybersecurity Education (NICE) but there may not be a need to maintain this in the framework. ***International Aspects, Impacts, and Alignm***ent is critical, but this should be handled within the Introduction to the Framework rather than kept within the Roadmap document. That would leave ***Technical Privacy Standards*** as the remaining item from the original Roadmap. Finally, we recommend adding ***Internet of Things*** as a roadmap issue, and in doing so we recommend that NIST define the term to encompass industrial and consumer devices/technologies.

API also submitted several recommended changes to the CSF in our response to the December RFI. We have included the most relevant of the open ones in attachments to this response.

Sincerely,
Aaron Padilla Senior Advisor, International Policy

1. API Comment:
   The current Framework lacks a mapping for the regulatory requirements of different government agencies
   Action:
   A separate guidance document should be composed to provide such mappings (if needed).

2. API Comment:
   The "Tiers" concept should be eliminated or restructured into something more meaningful/useful.
   Action:
   Tiers are selected for the organization as a whole. This ostensibly guides the creation of profiles but an organization may not aspire to have each and every control meet the same maturity level. For example, some controls, perhaps around critical infrastructure or data, will need to exceed the organizational tier.

   A company's tier selection may give a general idea of philosophy but would or could mask actual control implementation (which is likely of more importance if someone is assessing a potential partner).

3. API Comment:
   Other authoritative sources should be reviewed to ensure complete coverage of references. One example is to add COBIT 5 APO13.12 as an informative reference to ID.GV-2.
   Action:
   Informative references should be updated.

4. API Comment:
   New subcategory proposed: ID-AM-7: Documentation (for software, hardware, devices, procedures, networks, diagrams and dataflows) is identified and inventoried.
   Action:
   Include new subcategory in draft.

5. API Comment:
   New subcategory proposed: PR.PT-6: Unnecessary applications and services are removed/disabled to reduce attack surface.
   Action:
   Include new subcategory in draft

6. API Comment:
   Awareness & Training could benefit from being made more prominent.
   Action:
   Include text that states that awareness/education is sprinkled through the document and consequently identifies the importance of this item.

7. API Comment:
   Aligning the implementation tiers to a commonly recognized maturity model (like CMMI) would help industry understand current capability levels and make smarter decisions. It would also fit with most other similar assessments and avoid the potential for confusion over implementation tiers and maturity.
   Action:
   Rather than include in the CSF proper, mappings between the CSF and other standards should be handled in supplementary documentation. Department of Energy did this with C2M2 by including a mapping to the NIST CSF core in the DOE CSF Guidance document.

8. API Comment:
   Corporate vs. Non-corporate devices is not addressed for asset management.
   Action:
   NIST should explicitly state that “within organizations” includes both corporate and non-corporate devices.

9. API Comment:
   Need clarity on whitelisting. Higher level of maturity would include whitelisting.
   Action:
   This guidance should be in supplementary documentation (if needed) and not included in CSF.

10. API Comment:
    No specification for how often asset management activities are to occur. "On a regular basis" is not descriptive enough.
    Action:
    This guidance should be in supplementary documentation (if needed) and not included in CSF.

11. API Comment:
    Relevant external parties/third parties are not defined.
    Action:
    Use this definition: “Third Parties are external organizations including vendors, contractors, cloud providers and other service providers where access is based upon a restricted trust model.”

12. API Comment:
    Risk Assessments for the Cloud environment are not discussed.
    Action:
    Preference is to avoid creating sections on different technologies or environments. If a cloud section is added, then one conceivably could add a section covering mobility and another on IoT and another on quantum computing. Over time the CSF would degenerate into a disjointed set of subcategories within different context.

    The generic sub-categories should be used for these different environments. Risk assessment for “cloud” or “supply chain” may need to cover some specific items, but in either case, a risk assessment is a risk assessment and the “risk assessment” sub-category can handle. If there are special items to be covered, then a sub-category can be added but within the appropriate function.

13. API Comment:
    No discussion of Federation or Federation architecture.
    Action:
    This guidance should be in supplementary documentation (if needed) and not included in CSF.

14. API Comment:
    A Network Protection/VPN-Firewall Reference Architecture is needed.
    Action:
    This guidance should be in supplementary documentation (if needed) and not included in CSF.

15. API Comment:
    No discussion of encryption standards.
    Action:
    This guidance should be in supplementary documentation (if needed) and not included in CSF.

16. API Comment:
    No discussion of key ownership.
    Action:
    This guidance should be in supplementary documentation (if needed) and not included in CSF.

17. API Comment:
    Cabling security discussion is incomplete.
    Action:
    This guidance should be in supplementary documentation (if needed) and not included in CSF.

18. API Comment:
    Incomplete discussion of secure backups.
    Action:
    Change PR.IP-4 to
    PR.IP-4: Backups of information are conducted, maintained, secured, and tested periodically

19. API Comment:
    No thresholds for triggering alerts were documented.
    Action:
    This guidance should be in supplementary documentation (if needed) and not included in CSF.

20. API Comment:
    No discussion of breach notifications from third parties.
    Action:
    The privacy / civil liberties section should be updated to include text covering working with third parties.

21. API Comment:
    How privacy regulations apply to third parties is not discussed.

22. API Comment:
    No mention of incident coordination with a third party.

23. API Comment:
    Inadequate discussion of guidelines for response communications with third parties. They are adequate for an internal response function.

24. API Comment:
    A self-assessment tool would be a helpful addition.
    Action:
    This guidance should be in supplementary documentation (if needed) and not included in CSF.

25. API Comment:
    To reduce risk of unauthorized access and compromise are: employing multi-factor authentication to critical devices and employing NAC (network access control) to limit devices on the network through recognition of authorized devices where practical.

Action:
This guidance should be in supplementary documentation (if needed) and not included in CSF.