AEM
Association of
Equipment Manufacturers

Headquarters
[redacted]

aem.org
aem@aem.org
☎ [redacted]

Cherilyn Pascoe
NIST Cybersecurity Framework Program Lead
cyberframework@nist.gov

Re: Public Draft: The NIST Cybersecurity Framework 2.0 National Institute of Standards and Technology

Dear Ms. Pascoe:

The Association of Equipment Manufacturers (AEM)[1] appreciates the opportunity to comment on the National Institute of Standards (NIST) *Public Draft: The NIST Cybersecurity Framework 2.0 National Institute of Standards and Technology,*[2] hereafter referred to as the Public Draft. We look forward to sharing the expertise and technical knowledge of our industry. We believe it is critically important when developing public policy, that the interests of all stakeholders be considered and understood.

The non-road equipment manufacturing industry understands the value and importance of developing a robust corporate cybersecurity framework. AEM will strive to provide technically sound information on these policymaking discussions going forward.

NIST Cybersecurity Framework (CSF) 2.0 Proposed Changes

AEM's member companies reviewed the public draft and offer the following changes:

CSF 2.0 GV.OV-01: Appendix C, Table 5: Include emphasis on establishing a risk tolerance level for the organization.

- This section needs to establish an overall risk tolerance level for the entire organization. Some business units may have a higher risk tolerance level than others. So, it's important to establish a baseline so the actions of one individual cannot subvert the operations of the entire company.
- To achieve this goal, AEM recommends that NEST specifically outlines this provision in the document.

ID.AM-05: Appendix C, Table 6: Include ownership for assets.

- This section needs to firmly establish the ownership of a business asset to ensure the potential issues are addressed by the appropriate party. With this line of responsibility established, the company can ensure any issue is properly addressed.

[1] AEM is the North American-based international trade group representing heavy-duty non-road equipment manufacturers and suppliers with more than 1,000 member companies and over 200 product lines in the construction, agriculture, mining, forestry and utility industries. The equipment manufacturing industry in the United States supports 2.8 million jobs and contributes roughly $288 billion to the economy every year. Our industries remain a critical part of the U.S. economy and represent 12 percent of all manufacturing jobs in the United States. Our members develop and produce a multitude of technologies in a wide range of products, components, and systems that ensure heavy-duty non-road equipment remains safe and efficient, while at the same time reducing carbon emissions and environmental hazards. Finished products have a life cycle measured in decades and are designed for professional recycling of the entire product at the end of life. Additionally, our industry sectors strive to develop climate friendly propulsion systems and support robust environmental stewardship programs around the world.

[2] https://csrc.nist.gov/News/2023/nist-releases-cybersecurity-framework-2-0-draft

DE.CM: Appendix C, Table 8: The definition of "Continuous Monitoring" has changed (from 800-53A, Rev 4), and should be fully defined in this context.

- AEM Recommends that NIST fully define and flesh out this concept.

DE.AE-04: Appendix C, Table 8: The scope of impact must be pre-determined. Organizations waiting until an event happens is too late.

- AEM requests more clarity from NIST on whether this section is addressing adverse events that have already happened or is this intended to look for potential future adverse events.
- The text implies that it's a previous event, but this is not stated. Perhaps there should be a separate goal detailing the response to an event that happened. This issue could go into section RS - (Respond Section – Incident reports are triaged and validated by the organization)

RS.MA-04: Appendix C, Table 9: Incident declaration role and criteria must be fully defined due to potential legal implications. This issue could be emphasized in GV.PO

- The rush to declare an incident can create significant legal implications. There needs to be an objective (perhaps in GV) that requires us to determine who should declare an incident as well as provide fully details criteria for making any such declaration.
- If this process is fully detailed, the result should help with potential insurance issues as well.

PR.DS-9: Appendix C, Table 7: Data is identified/classified with handling paradigms consistent with risk tolerance.

- AEM recommends that NIST reference the Governance section and place more emphasis on the how and they why (data handling with an emphasis on risk management).

PR.DS-10: Appendix C, Table 7: Data-in-use might be better explained as "while processed" this seems redundant with 01, or 02.

- Data-in-use is not a term that is an industry standard term. Would be better to use words that build clarity with the reader.

Summary of Requests:

AEM appreciates the opportunity to comment on the Public Draft. The equipment manufacturing industry recognizes the importance of establishing reobust processes and procedures for building out the nation's cybersecurity infrastructure. Additionally, equipment manufacturers understand the value in working more closely with NIST to communicate the needs of industry during crucial policymaking decisions. To ensure new rules meet their objectives with accurate and complete data, AEM requests that NIST give consideration to the comment recommendations contained in this comment.

AEM Appreciates your consideration of these comments.

Please feel free to contact Jason Malcore, AEM's Senior Director, Safety & Product Leadership at [redacted] if you have any questions or require any further information.

Best Regards,

Jason Malcore
Senior Director – Safety & Product Leadership
Association of Equipment Manufacturers (AEM