American Property Casualty Insurance Association
INSURING AMERICA apci.org

NAMIC®
NATIONAL ASSOCIATION OF MUTUAL INSURANCE COMPANIES

November 3, 2023

Via email: cyberframework@nist.gov
Alicia Chambers
Executive Secretariat
National Institute of Standards and Technology
Gaithersburg, MD 20899

Re: NIST Cybersecurity Framework 2.0
Initial Public Draft (NIST CSWP 29)
Published August 8, 2023

Dear Ms. Chambers:

In response to the public comment draft of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, the American Property Casualty Insurance Association (APCIA) and the National Association of Mutual Insurance Companies (NAMIC), trade associations representing property-casualty insurers (joint trades), submit this letter jointly.

With its risk-based and systematic approach, the NIST CSF plays an important role in helping businesses – regardless of size – manage cybersecurity risks and threats and protect networks and data while also being appropriately flexible and adaptable. The CSF offers a valuable tool to aid a cybersecurity program. The joint trades largely support the draft changes reflected in the 2.0 version and this letter conveys input from member property-casualty insurers.

SPECIFIC VALUE-ADDED ADDITIONS TO THE UPDATED FRAMEWORK

The joint trades ask NIST to consider additions that would be helpful to guideline users:

Category – Organization Context (GV.OC)

- Subcategory – GV.OC-06:
  - Cybersecurity impacts to the organization's objectives are understood and the associated decisions are communicated appropriately.

Category – Risk Management Strategy (GV.RM)

- Subcategory – GV.RM-09:
  - Defined measures and reporting that provides visibility into risk posture and status of accepted or in progress risks.

- Subcategory – GV.RM-10:
    - Risk key terms, definitions, and taxonomies are documented and communicated as part of risk management education and programming.
- Subcategory – GV.RM-11:
    - Additional considerations for higher-risk geographies; mergers and acquisitions are addressed in the overall risk management strategy and plan.

Category – Oversight (GV.OV)

- Subcategory – GV.RM-08:
    - A consistent and repeatable process for measuring and reporting the risk management program through OKRs, KPIs and KRIs.

Category – Incident Management (RS.MA)

- Subcategory – RS.MA-06:
    - Incident training is conducted for appropriate stakeholders on a periodic basis, based on risk.

EXPANDING CONSIDERATIONS FOR UPDATED FRAMEWORK

The joint trades ask NIST to consider the following additional ways to enhance guidance:

Corrective Action & Disciplinary Policies

- Provide for corrective action and disciplinary policies that focus on cyber security policy violations.
    - Examples – Corrective action policies for security policy violations are documented, communicated, and provided as part of the general security awareness and training programs.
    - Examples – Governance and measures for security policy violations are documented and reviewed as part of the security metrics program and performance management systems.

Higher-Risk Geographies

- Include some guidance or content relating to higher risk geographies.
    - Examples – Monitoring controls are in place commensurate with the geographical risks.

Risk-Based Proportionality & Staffing

- Insert a statement that organizations staff their information security program and function commensurate with their risk posture, size, products, and services.
    - This could clarify that there is not a one-size-fits all single best approach to staffing these areas because the risks relating to the complexity of the entity and the nature and scope of their activities may vary.

* * * * *

In closing, the joint trades appreciate the collaboration built-into the NIST cybersecurity framework development and revision process. The NIST CSF 2.0 is intended to bring together meaningful cybersecurity risk and vulnerability management and workability. Thank you for your consideration of the suggestions offered here.

Respectfully,

Shelby Schoensee
Director, Cyber Issues
American Property Casualty
Insurance Association

Thomas Karol
General Counsel, Federal
National Association of Mutual Insurance
Companies