June 9, 2023

National Institute of Standards and Technology (NIST)
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

RE: Discussion Draft of the NIST Cybersecurity Framework 2.0 Core

Greetings NIST,

Thank you for the opportunity to provide feedback on the NIST Cybersecurity Framework 2.0 Core. Recommendations have been outlined on subsequent pages, with initial suggested changes in italicized blue font; additional feedback has been highlighted in yellow.

Sincerely,

Nicole Rohloff

Nicole Rohloff

2.0 Implementation Example (New Example Proposed)

- PR.PS-02: Software incompatibilities are identified and addressed to ensure routine patching can be conducted as scheduled (new example)

2.0 Implementation Example(s) (Proposed Revision to Current Example)

- Example 2: DE.AE-07: Information from asset inventories is securely provided to detection technologies, processes, and personnel (current)
    - Example 2: DE.AE-07: Information from asset inventories is *collected, updated,* and securely provided to detection technologies, processes, and personnel (proposed revision)

2.0 Category and Subcategory Recommended Changes

CSF 2.0 Function: Govern | Category: Organizational Context: (GV.OC)

- Subcategory GV.OC-01: Organizational mission is understood in order to prioritize cybersecurity risk management (current)
    - Proposed GV.OC-01: Organizational strategy, mission, and *priorities are established and communicated to internal stakeholders to aid in the prioritization* of cybersecurity risk management activities (proposed)
- Subcategory GV.OC-02: Internal and external stakeholders, and their expectations regarding cybersecurity risk management, are determined (current)
    - Proposed GV.OC-02: Internal and external stakeholder *expectations regarding* cybersecurity risk management *are established, understood, and proactively managed (e.g., stakeholders may include the Chief Risk Officer, management team, board members, etc.).*

CSF 2.0 Function: Govern | Category: Risk Management Strategy: (GV.RM)

- Current GV-RM: The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established and used to support operational risk decisions (current)
    - Proposed (GV.RM): The organization's plan for managing risk including, assessment, response, and monitoring. A risk management strategy provides framework that helps improve operational effectiveness, and aids in risk reporting and decision-making at all levels within the organization (note: in alignment with current NIST definition: https://csrc.nist.gov/glossary/term/risk_management_strategy)

- Subcategory GV.RM-01: Cybersecurity risk management objectives are established and agreed to by organizational stakeholders (current)
    - Proposed GV.RM-01: Cybersecurity risk management objectives are established, *understood, and managed to ensure organizational alignment with internal and external stakeholders.*

- Subcategory GV.RM-02: Cybersecurity supply chain risk management strategy is established, agreed to by organizational stakeholders, and managed (current)
    - Proposed GV.RM-02: Supply chain risk management (SCRM) strategy is established, *understood, and managed – in accordance with regulations, guidelines, directives, policies, and/or Executive Orders, as applicable.*

- Subcategory GV.RM-04: Cybersecurity risk management is considered part of enterprise risk management (current)

  - Proposed GV.RM-04: Cybersecurity risk management *activities are integrated with the organization's enterprise risk management (ERM) program*. Note: recommend inserting footnote that links to 8286.

- Subcategory GV.RM-07: Risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks (current)
  - Proposed GV.RM-07: Risk management strategy is *established,* reviewed, and adjusted to ensure organizational requirements and risks are *understood and processes are executed consistently.*

- Subcategory GV.RM-08: Effectiveness and adequacy of cybersecurity risk management strategy and results are assessed and reviewed by organizational leaders (current)
  - Proposed GV.RM-08: Effectiveness and adequacy of cybersecurity risk management strategy *and outcomes* are assessed, reviewed, and *governed* by risk management teams(s), organizational leaders, and/or other key stakeholders.

CSF 2.0 Function: Govern | Category: Roles and Responsibilities (GV.RR)

- Subcategory GV.RR-01: Organizational leadership takes responsibility for decisions associated with cybersecurity risks and establishes a culture that is risk-aware, behaves in an ethical manner, and promotes continuous improvement (current)
  - Proposed: Organizational leadership takes responsibility *for cybersecurity risk and fosters a culture that is proactive, collaborative, risk-aware, ethical, and aims to continuously improve.*

- Subcategory GV.RR-02: Roles and responsibilities related to cybersecurity risk management are established and communicated (current)
  - Proposed GV.RR-02: Roles and responsibilities related to *cybersecurity and supply chain risk management* are established and communicated to internal stakeholders.

- Subcategory GV.RR-03: Roles and responsibilities for customers, partners, and other third-party stakeholders are established and communicated (current)
  - Proposed GV.RR-03: Roles and responsibilities for *cybersecurity and supply chain risk management* are established *and communicated to customers, partners, and other third-party stakeholders.*

- Subcategory GV.RR-04: Roles and responsibilities for suppliers are established, documented in contractual language, and communicated (current)
  - Proposed GV.RR-04: Roles and responsibilities for *cybersecurity and supply chain risk management* are established, clearly documented in contractual language in accordance with federal, state, local, and/or internal guidelines, communicated *to suppliers and updated as appropriate.*
  -

- Subcategory GV.RR-05: Lines of communication across the organization are established for cybersecurity risks, including supply chain risks (current)

- Proposed GV.RR-05: Lines of communication for *cybersecurity and supply chain risk* are established and maintained across the organization to ensure alignment, timely action and reporting to key stakeholders.

- Subcategory GV.RR-06: Resourcing and authorities for cybersecurity are decided commensurate with risk strategy, roles, and policies (current)
  - Proposed GV.RR-06: Resourcing and authorities for cybersecurity are decided commensurate with risk strategy, *business needs*, *priorities, and* policies.

- Subcategory GV.RR-07: Cybersecurity is included in human resources practices (e.g., training, deprovisioning, personnel screening) (current)
  - Proposed GV.RR-07: Cybersecurity is incorporated in human resources practices (e.g., training, deprovisioning, personnel screening, *onboarding and offboarding*).

CSF 2.0 Function: Govern | Category Policies and Procedures (GV.PO)

- Subcategory GV.PO-01: Policies, processes, and procedures for managing cybersecurity risks are established based on organizational context, risk management strategy, and priorities and are communicated (current)
  - Proposed GV.PO-01: Policies, processes, and procedures for managing cybersecurity risks are established *and communicated by organizational leaders based on enterprise mission, organizational context, business priorities, and risk management strategy.*

- Subcategory GV.PO-03: Policies and procedures are reviewed, updated, and communicated to reflect changes in requirements, threats, technology, and organizational mission (current)
  - Proposed GV.PO-03: Policies, *processes,* and procedures are reviewed, updated, and communicated to reflect changes in requirements, threats, technology, and/or organizational mission.

CSF 2.0 Function: Identify | Category: Asset Management

- Subcategory ID.AM-03: Representations of the organization's authorized network communication and network data flows are maintained (current)
  - Proposed ID.AM-03: Representations of the organization's authorized network communication and network data flows are *identified and* maintained.

- Subcategory ID.RA-04: Potential business impacts and likelihoods are identified and recorded (current)
  - Proposed ID.RA-04: Potential business impacts and likelihoods are identified, recorded, and *communicated with key stakeholders and/or business areas.*

- Subcategory ID.RA-10: Exceptions to security measures are reviewed, tracked, and compensated for (current)
  - Proposed ID.RA-10: Exceptions to security measures are *identified*, reviewed, tracked, and *addressed.*

- NEW Proposed subcategory: *ID.RA-11: Security gaps (i.e., findings) are identified,* assessed, analyzed, *tracked, and addressed.*

- Subcategory ID.SC-03: Cybersecurity requirements are integrated into contracts with suppliers and third-party partners (current)
    - Proposed ID.SC-03: Cybersecurity requirements are outlined and integrated in *supplier and third-party contracts, agreements, purchase orders, etc.*

- Subcategory ID.IM-01: Continuous evaluation, including through reviews, audits, and assessments (including self-assessments), is applied to identify opportunities for improvement across all Framework Functions (current)
    - Proposed ID.IM-01: Continuous evaluation *is incorporated in the organization's business operations to identify opportunities for improvement across all framework functions, including reviews, audits, and assessments (e.g., gap analysis).*

- Subcategory ID.IM-03: Improvements for processes and activities across all Framework Functions are identified based on lessons learned (current)
    - Proposed ID.IM-03: Improvements for processes and activities across all Framework Functions *are identified based on continuous evaluation outputs (e.g., reviews, audits, lessons learned, etc.).*

CSF 2.0 Function: Protect | Category: Awareness and Training

- Awareness and Training (PR.AT): The organization's personnel and third-parties are provided cybersecurity awareness and training to perform their cybersecurity-related tasks consistent with related policies, procedures, and agreement (current)
    - Proposed Awareness and Training (PR.AT): *Cybersecurity role-based training (RBT) for personnel and third parties is provided to ensure cybersecurity-related tasks are performed in accordance with related policies, procedures, and agreements.*