Subject: Feedback on the NIST Cybersecurity Framework (CSF) 2.0

Dear NIST Team,

Thank you for the opportunity to provide feedback to the NIST CSF 2.0.

Introduction

The goal of this feedback is to strengthen the ties between Section 3., Using the Framework, and Appendix C, Framework Core regarding Cybersecurity Supply Chain Risk Management (C-SCRM). Section 3.5, Managing Cybersecurity Risk in Supply Chains with the Framework, Lines 586 to 588 state "…provide a source for the organization to consider as a basis for supplier cybersecurity requirements, both for direct suppliers and as flow-down requirements for lower-tier suppliers [GV.SC-05]." The identification of flow-down requirements for lower-tier suppliers is an important consideration that should be explicitly stated in the relevant elements of Appendix C.

Suggested Modifications

- GV.SC-05. Modify the text to incorporate the text shown in bold: "Requirements to address cybersecurity risks in supply chains **(including lower tier suppliers)** are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties (formerly ID.SC-03)"
- GV.SC-07 Modify the text to incorporate the text shown in bold to better align with the wording from NIST Special Publication (SP) 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations Page 1, Section 1, Paragraph 4, lines 1-3: "The risks posed by a supplier, **their supply chains**, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship (formerly ID.SC-02, ID.SC-04.)

Sincerely,

Vince Minerva