Control Risks Group, L.L.C.
[redacted]

[redacted]
controlrisks.com

General

National Institute of Standards and Technology
U.S. Department of Commerce

May 25, 2023

Feedback regarding the Discussion Draft of the NIST Cybersecurity Framework 2.0 Core

NIST Cybersecurity Framework Program,

Control Risks is a boutique special risks consultancy firm with offices worldwide postured to meet the needs of our global client base. Originating in the kidnap and recovery space, Control Risks has expanded over the past five decades into the worlds of physical, digital, and regulatory risk while continuing to place threat-informed risk understanding at the core of our methodologies and approaches. The Digital Risks Team at Control Risks leverages the NIST Cybersecurity Framework (CSF) regularly with clients across the globe to enable them to both better understand their current program maturity levels, as well as to assess target maturity levels based on analysis of the most likely threats they face in the digital domain.

Our collective team greatly appreciates the opportunity to review and provide feedback on the program's CSF 2.0 Core. It is our pleasure to submit the following recommendations for consideration:

- **GV.OC-04**: We recommend that the program re-introduce language regarding the identification of dependencies between business services would better align with the prominence of supply chain cyber attack techniques what may impact organizational operations further upstream.
- **GV.OC-05**: We recommend introducing language that also encourages organizations to determine and communicate their potential role as a supplier to other businesses as a formal process.
- **GV.RM-04**: We recommend replacing the phrase "considered part of" with "integrated into" so reflect a need for an active engagement between cyber risk managers and enterprise risk managers within an organization.
- **GV.RR-02**: We recommend adding language regarding roles and responsibilities being tested and rehearsed regularly, in addition to being established and communicated. This recommendation originates from our work with clients who have cyber response plans and procedures codified; however, when we facilitate exercises with their leadership teams, it becomes apparent that individuals are unfamiliar with what is expected of them during a cyber crisis.
- **GV.PO-02**: We recommend a more nuanced approach to the application of internal cyber security policies to supplies as different vendors likely require more tailored oversight of digital risks to organization. Additionally, the level of inspection and audit that is plausible for internal systems and processes may not be feasible to apply to suppliers from a resource or budget perspective.
- **ID.RA-02**: We recommend incorporating language that reflects the need to both receive cyber threat intelligence but also to integrate it into the organization's enterprise risk management process, to include

threat management and vulnerability management. This recommendation originates from our work with clients who have access to cyber threat intelligence feeds but are looking for advise as to how to operationalize those feeds to inform risk management processes and decision points within their organizations.

- **PR.IR-01**: We recommend adding language regarding plans being tested and rehearsed regularly, in addition to being communicated and maintained. This recommendation originates from our work with clients who have cyber response plans and procedures codified; however, when we facilitate exercises with their leadership teams, it becomes apparent that individuals are unfamiliar with what is expected of them during a cyber crisis.
- **RC.RP-03**: We recommend language that reflects more regular verification of backups rather than only prior to using them for restoration. As backups continue to be one of the most effective security controls for mitigating the risks from ransomware, it has become ever-more critical to ensure integrity and availability of backups on a frequent basis.

Respectfully submitted,

Control Risks
Global Digital Risks Team

POC: Steven Sacks
[redacted]