Capital One Financial Corporation
[redacted]

March 3, 2023

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

Re: NIST–2023–0001, NIST Cybersecurity Framework 2.0 Concept Paper

Capital One Financial Corporation ("Capital One") commends NIST for the significant undertaking of initiating NIST Cybersecurity Framework (CSF) 2.0.[1] NIST captured a comprehensive picture of the changing needs of the cybersecurity community and an approach to begin addressing them within the CSF. As Capital One reviewed the *NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework*, there were a few areas that we urge NIST to further explore as development of the CSF 2.0 progresses.

NIST CSF at Capital One

As Capital One detailed in our April 12, 2022 response to the *Notice and Request for Comment on Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management*, the NIST CSF is an essential resource that supports our cybersecurity governance and risk management activities. Our company relies broadly upon the CSF, and, in particular, has made it the foundation of our enterprise cyber maturity assessment program.

Capital One leverages the CSF as the initial structure for our internal cyber maturity assessment program by identifying and mapping approximately 1,000 cyber capabilities, 400 of which are unique capabilities, to the 108 NIST CSF subcategories. Linking specific capabilities to each subcategory enables a consistent and complete approach when performing cyber maturity

[1] Capital One Financial Corporation (www.capitalone.com) is a financial holding company which, along with its subsidiaries, had $333.0 billion in deposits and $455.2 billion in total assets as of December 31, 2022. Headquartered in McLean, Virginia, Capital One offers a broad spectrum of financial products and services to consumers, small businesses and commercial clients through a variety of channels. Capital One, N.A. has branches located primarily in New York, Louisiana, Texas, Maryland, Virginia, New Jersey and the District of Columbia. A Fortune 500 company, Capital One trades on the New York Stock Exchange under the symbol "COF" and is included in the S&P 100 index.

assessments over time. For each of the unique capabilities, we also documented key characteristics of maturity at Tier 1: Partial through Tier 4: Adaptive.

Given the rapid evolution of both cyber threats and best practices for mitigation, we periodically review and validate capability maturity descriptors to ensure they stay current. Having clearly-defined and up to date maturity descriptors for Tiers 1 to 4 has enhanced our ability to develop targeted maturity goals in line with business objectives and the evolving threat landscape. As we look to further mature our program, Capital One is looking for industry best practices surrounding performance metrics to improve measurement tactics, gain indicators of change, and be able to adapt the model more quickly.

In addition, we value the ability to map controls between the CSF and other industry-standard resources, such as NIST Special Publication 800-53. Aligning industry standards and procedures with the CSF has helped Capital One validate the scope of cyber governance in place as well as the maturity of the control environment. A standard set of controls, whether across multiple frameworks or centralized, provides Capital One the confidence to know that a minimum cybersecurity threshold is covered. This enables the organization to focus on advancing maturity and protecting against more sophisticated adversaries.

Proposed Considerations

While the CSF already demonstrates many strengths, Capital One appreciates the opportunity to contribute comments for NIST's consideration regarding future enhancements. As an avid consumer of the CSF, we would like to highlight the following areas for NIST consideration:

- Capital One strongly recommends that a standardized approach to maturity scoring remain a topic of consideration for NIST CSF 2.0. As the use of the CSF continues to expand, a standardized scoring scale would help organizations benchmark themselves across the industry and allow for a more accurate comparison from independent third party assessments. Additionally, the inclusion of performance metrics within the framework could help organizations adapt to a quickly changing threat landscape faster, as a complete refresh would not be needed but simply a shifted metrics lens.

  For example, Capital One's current methodology to measure cybersecurity maturity against the CSF includes:
  - A four tier scoring model - Partial, Risk Informed, Repeatable, and Adaptive
  - Subcategories are broken down further into capabilities which define key components within a subcategory. For example, "*PR.AC-5: Network integrity is protected*" is further broken down into capabilities such as firewall configuration, and firewall rule management. This provides a level of standardization and consistency as personnel change over time.

- Maturity descriptors define what is expected to achieve at each level of maturity specific to the capabilities
- Regular assessments of the cyber program against this scoring criteria provide a maturity score and targeted recommendations in line with the evolving threat landscape

We believe the creation of a standardized approach to maturity scoring would be the single most significant action NIST could take to increase the value and impact of the CSF.

- Capital One recommends the addition of a standard control inventory to highlight the importance of cybersecurity control governance. As NIST looks to clarify the relationship between governance and cybersecurity risk management, this addition could be an ideal opportunity to further enhance the relationship between the CSF and NIST 800-53 by leveraging the latter as a foundational control inventory. This addition would help CSF users better manage an increasing volume of self-identified controls and inform strategic decision making.

- As NIST looks to further emphasize the importance of cybersecurity supply chain risk management (C-SCRM), Capital One agrees with this expansion and its criticality in protecting organizational assets. Capital One encourages NIST to consider integrating C-SCRM outcomes throughout the CSF Core across Functions with a majority added to the existing Identify - Supply Chain Risk Management (ID.SC) category. Specifically, C-SCRM 'Enhancing Practices' are not thoroughly captured within the CSF, including topics such as process automation, quantitative risk analysis, and predictive strategies. The inclusion of all C-SCRM practices referenced in NIST 800-161 would allow for more comprehensive coverage in the Supply Chain Risk Management category of the CSF.

- As part of any future update of the NIST CSF, Capital One would welcome additional focus on the subcategories related to network security. While having significant impact on the overall cyber posture of the organization, several key topics are concentrated in a relatively small number of subcategories. A few examples of areas that we would encourage NIST to consider expanding both breadth and depth include (but are not limited to): network segmentation and microsegmentation; firewall management and configuration; application permit listing; network access control; proxy management; and environment isolation.

- As we strive to increase synergies between our cyber maturity program and other cyber functions, Capital One would welcome further efforts by NIST to develop supporting resources that align the CSF with the MITRE ATT&CK® framework. A NIST-validated resource would benefit our internal program as we assess and make risk-informed recommendations for strengthening cybersecurity mitigation measures.

Capital One looks forward to continuing to engage with NIST on this important topic and looks forward to additional conversations on how to ensure the CSF remains the premier approach for organizations seeking to improve and evaluate their cybersecurity maturity.

Sincerely,

DocuSigned by:

Chris Betz

CB355DA4EEAF41A...

Chris Betz, Executive Vice President, Chief Information Security Officer

DocuSigned by:

Andy Ozment

154DF8036C8A421...

Andy Ozment, Executive Vice President, Chief Technology Risk Officer