



Capital One Financial Corporation
1600 Capital One Drive
McLean, Virginia 22102

April 12, 2022

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

Re: NIST–2022–0001, NIST Cybersecurity RFI

Capital One Financial Corporation (“Capital One”) welcomes the opportunity to contribute to the Notice and Request for Comment on Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management.¹ Capital One values NIST’s demonstrated commitment to providing broadly-applicable frameworks and associated resources for entities of all sizes, public and private, to use when designing, operating, and continuously improving cybersecurity programs. Given the importance of sector- and industry-spanning approaches to combating cyber threats, NIST’s leadership in maintaining the Cybersecurity Framework (“CSF”) represents an important public service.

Capital One recommends that NIST initiate a process to update the CSF. It is critical that the NIST framework keeps pace with the ever-evolving nature of both technology and cybersecurity threats and in turn retains its relevance to the many organizations that rely on it.

NIST CSF at Capital One

For Capital One, the NIST CSF is an essential resource that supports 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.

¹ Capital One Financial Corporation (www.capitalone.com) is a financial holding company whose subsidiaries, which include Capital One, N.A., and Capital One Bank (USA), N.A., had \$311.0 billion in deposits and \$432.4 billion in total assets as of December 31, 2021. 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.

We find the CSF's focus on all stages of the cybersecurity event lifecycle helpful in ensuring a comprehensive approach to evaluating maturity. To bring the CSF to life as part of our internal cyber maturity assessment program, Capital One identified and mapped over 400 unique cyber capabilities to the 108 NIST CSF subcategories. Linking specific capabilities to each subcategory enables a consistent and complete approach when performing cyber maturity assessments over time. For each of the unique capabilities, we also documented key characteristics of maturity at Tier 1: Partial through Tier 4: Adaptive. This effort was strengthened through review and challenge across multiple risk offices and lines of defense working in partnership.

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 share targeted recommendations with teams striving toward "next level" maturity goals.

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 cyber 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. The CSF provides a consistent and repeatable basis for assessing cyber maturity at both enterprise and individual business unit scale. This has served to inform and further strengthen internal governance and risk management decision-making.

The wider CSF-supporting ecosystem of cyber-related resources NIST provides is useful for other cyber risk management purposes as well. For example, Capital One continues to leverage the National Initiative for Cybersecurity Education (NICE) framework as a tool for cyber career planning and development at both individual and programmatic (i.e., labor strategy) levels.

The NIST CSF also plays a key role in how we aggregate and communicate insights to stakeholders at many levels, from line performers to senior executives and the board of directors. Broadly speaking, Capital One continues to pursue a significant technology transformation agenda that supports our business goals within a defined risk management framework. Capital One is investing substantial resources to ensure the strength of our cyber defenses, in line with customer, leadership and regulator expectations. The NIST CSF plays a key role in our processes for prioritizing investments in new capabilities and strengthening existing capabilities in response to the evolving cyber threat landscape. To enable leadership decision-making, we have developed a set of cyber risk scenarios that distinctly correlate to CSF-aligned capabilities. The end result is to ensure we are meeting the highest standards of protection for our customers.

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:


- Given the continued rapid advance of cloud-based computing solutions for organizations across all industries and sectors, Capital One encourages NIST to consider updates to the CSF that more fully define control environment maturity models for the full range of cloud architectures, including but not limited to private, hybrid, public, and community cloud deployments.
- 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.
- We recommend NIST continue to adopt, refine, and promote industry-specific profiles, such as the Financial Services sector-specific cybersecurity “profile” developed by the Financial Services Sector Coordinating Council. These profiles feature risk-informed guidance on the importance of and/or appropriate weighting to assign specific cyber capabilities aligned to each of the 108 CSF Subcategories. The goal would be to provide additional guidance to users in these sectors that appropriate capabilities are in place and operating at recommended levels relative to both threats and industry best practices. Where sensible, we encourage NIST to incorporate broadly applicable aspects of these profiles into the CSF itself.
- Capital One is aware of a proposed new Function specifically dedicated to cyber Governance. While we have been able to successfully operate our program with governance topics largely subsumed within the Identify function, we believe a Governance-specific function offers several benefits. Formalizing a Governance Function would ensure audiences consuming maturity scores and reporting at the Function level consistently see reporting on this key area. It would also allow for additional focus on evolving areas of best practice, for example cybersecurity oversight.
- 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 would welcome any innovation NIST can provide related to standardizing metrics for common cyber topics. This would pertain specifically to

areas almost every organization’s cyber programs typically seek to track and report on, such as vulnerability management, access management, and incident management. NIST is uniquely well-positioned to provide a powerful voice for standardizing best practices regarding metrics. Having at least one standardized approach for measuring these areas endorsed by NIST would prove extremely valuable.


- Finally, Capital One would value a deeper understanding of other users’ experiences with the CSF’s four-tier maturity model. When assessing internal cyber maturity and reporting results to leadership, our experience has frequently involved discussions on “partial” scores that fall in between the four established tiers. Adding additional tiers might enable more nuanced discussions, albeit at the cost of greater complexity and potentially disrupting the ability to compare current with previous scores (in the event of changes to the scoring model). Alternatively, we would welcome additional guidance regarding best practices when communicating and making decisions using partial scores.

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:

CB355DA4EEAF41A...

Chris Betz, SVP, Chief Information Security Officer

DocuSigned by:

154DF8036C8A421...

Andy Ozment, EVP, Chief Technology Risk Officer