ECKERT SEAMANS ATTORNEYS AT LAW

May 2024

Cybersecurity, Data Protection & Privacy Update

New Release of NIST Cybersecurity Framework 2.0

By Matthew H. Meade and Elizabeth Wilson

OVERVIEW

On February 26, 2024, the National Institute of Standards and Technology ("NIST") revamped its Cybersecurity Framework ("NIST CSF 2.0") to assist organizations in reducing risk when developing and managing their cybersecurity program[1]. The NIST CSF 2.0 guidance includes a new cybersecurity governance core function and emphasizes the importance of identifying and managing cybersecurity risks arising from an organization's supply chain[2]. NIST CSF 2.0 also provides organizations with a "suite of resources" to help organizations of all sizes and industries meet their cybersecurity goals[3]. Under Secretary of Commerce for Standards and Technology and NIST Director Laurie E. Locascio. "CSF 2.0, which builds on previous versions, is not just about one document. It is about a suite of resources that can be customized and used individually or in combination over time as an organization's cybersecurity needs change and its capabilities evolve[4]." "Developed by working closely with stakeholders and reflecting the most recent cybersecurity challenges and management practices, this update aims to make the framework even more relevant to a wider swath of users in the United States and abroad," according to Kevin Stine, chief of NIST's Applied Cybersecurity Division[5].

The suite of resources include:

1. The full NIST Cybersecurity Framework 2.0 including the (i) CSF Core, which is composed of core functions to consider when creating a cybersecurity program, (ii) CSF Organizational Profiles, which help describe an organization's current and target cybersecurity program posture, and (iii) CSF Tiers, which demonstrate the maturity of an organization's cybersecurity program;
2. An Organizational Profile Template;
3. Multiple Quick-Start Guides tailored to different organizational types (including small and medium sized organizations) to help them navigate NIST CSF 2.0;
4. Community Profile Examples offering common risk management guidance across different sectors or industries;
5. A Success Stories page providing real life examples of successful NIST CSF 2.0 implementation;
6. A Frequently Asked Questions page;
7. The CSF 2.0 Reference Tool allowing users to explore the CSF Core functions; and
8. Informative Reference Materials providing further guidance on how organizations can achieve the CSF Core functions.

[1] https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework.
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*

CSF CORE

The CSF Core in NIST CSF 2.0 is made up of 6 core functions that govern the lifecycle of an effective cybersecurity program including: (i) cybersecurity governance, (ii) identifying cybersecurity risk, (iii) protecting assets and data, (iv) detecting security vulnerabilities and cybersecurity incidents, (v) responding to cybersecurity incidents, and (vi) recovering from a cybersecurity incident. Each core function has underlying cybersecurity categories and subcategories meant to inform organizations on how to develop their cybersecurity program. A list of the core functions and a summary of the underlying categories is found below.

1) Govern[6]

a) *Organizational Context*. The organization seeks to understand the circumstances that may affect its risk management decisions such as its mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements.

b) *Risk Management Strategy*. The organization establishes, communicates, and uses its priorities, constraints, risk tolerance and appetite statements, and assumptions to support its operational risk decisions.

c) *Roles, Responsibilities, and Authorities*. The organization establishes and communicates its cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement.

d) *Policy*. The organization establishes, communicates, and enforces its cybersecurity policy.

e) *Oversight*. The organization uses the results of its organization-wide cybersecurity risk management activities and performance to inform, improve, and adjust its risk management strategy.

f) *Cybersecurity Supply Chain Risk Management*. The organization identifies, establishes, manages, monitors, and improves its cyber supply chain risk management processes.

2) Identify[7]

a) *Asset Management*. The organization identifies and manages its assets (e.g., data, hardware, software, systems, facilities, services, and people) in accordance with their relative importance to the organization's objectives and risk strategy.

b) *Risk Assessment*. The organization completes assessments to understand the level of cybersecurity risk to the organization, its assets, and individuals.

c) *Improvement*. The organization identifies improvements to its cybersecurity risk management processes, procedures, and activities.

[6] *See* U.S. Department of Commerce National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, February 26, 2024, at 16-18, *available at* https://www.nist.gov/cyberframework.
[7] *See Id.* at 18-19.

3) Protect[8]

a) *Identity Management, Authentication, and Access Control*. The organization limits and manages access to physical and logical assets to authorized users, services, and hardware based on the assessed risk of unauthorized access

b) *Awareness and Training*. The organization provides its personnel with cybersecurity awareness training so that they can perform their cybersecurity-related tasks.

c) *Data Security*. The organization manages its data in accordance with its risk strategy to protect the confidentiality, integrity, and availability of information.

d) *Platform Security*. The organization manages its hardware, software, and physical and virtual platforms in accordance with the organization's risk strategy to protect their confidentiality, integrity, and availability.

e) *Technology Infrastructure Resilience*. The organization manages its security architectures in accordance with its risk strategy to protect asset confidentiality, integrity, and availability, and ensure organizational resilience.

4) Detect[9]

a) *Continuous Monitoring*. The organization monitors its assets to find anomalies, indicators of compromise, and other potentially adverse events.

b) *Adverse Event Analysis*. The organization analyzes the identified anomalies, indicators of compromise, and other potentially adverse events to characterize the events and detect cybersecurity incidents.

5) Respond[10]

a) *Incident Management*. The organization responds to and manages detected cybersecurity incidents.

b) *Incident Analysis*. The organization investigates the incident to effectively respond to the incident and to support forensics and recovery activities.

c) *Incident Response Reporting and Communication*. The organization coordinates with internal and external stakeholders on incident response measures and responds to the incident in accordance with required laws, regulations, or policies.

d) *Incident Mitigation*. The organization performs incident mitigation activities to prevent the incident from expanding and to mitigate its harmful effects.

[8] *See Id.* at 19-21.
[9] *See Id.* at 21.
[10] *See Id.* at 22.

6) Recover[11]

a) *Incident Recovery Plan Execution*. The organization performs restoration activities to ensure operational availability of systems and services affected by the incident.

b) *Incident Recovery Communication*. The organization ensures that all restoration activities are coordinated with internal and external parties.

CSF ORGANIZATIONAL PROFILES AND CSF TIERS

The CSF Organizational Profile is intended to help organizations compare its cybersecurity program to the CSF Core functions. The CSF Organization Profile is composed of the organization's (i) "Current Profile" (e.g., how the organization is currently meeting the CSF Core functions) and (ii) "Target Profile" (e.g., the CSF Core functions the organization is working to achieve in the future).

The CSF Tiers are used to help organizations better understand the rigor of its CSF Organization Profile. There are four CSF Tiers: (i) Tier 1 – Partial, (ii) Tier 2 – Risk Informed, (iii) Tier 3 – Repeatable, and (iv) Tier 4 – Adaptive. The CSF tiers range from organizations that address cybersecurity risk from an "informal ad-hoc basis" ("Partial Tier 1") to mature cybersecurity programs that are "agile, risk-informed, and continuously improving" ("Adaptive Tier 4")[12].

HOW WE CAN HELP

ECKERT SEAMANS ATTORNEYS AT LAW

This Cybersecurity, Data Protection & Privacy Update is intended to keep readers current on developments in the law and is not intended to be legal advice. If you have any questions, please contact Matthew H. Meade at 412.566.6983 or mmeade@eckertseamans.com, Elizabeth Wilson at 215.851.8497 or ewilson@eckertseamans.com, a member of our Cybersecurity, Data Protection & Privacy Practice Group, or any other attorney at Eckert Seamans with whom you have been working for further information and assistance.

[11] *See Id.* at 22-23.
[12] *Id.* at 7-8.