The NIST Cybersecurity Framework - Version 1.0

On February 12, 2013, President Obama issued Executive Order (EO) 13636, directing the National Institute of Standards and Technology (NIST) to establish a "framework to reduce cyber risks to critical infrastructure," which was defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[1] President Obama required the framework to include "a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."[2] This framework was intended to provide a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" to manage cybersecurity risk.[3]

NIST subsequently hosted a series of workshops with stakeholders and solicited comments on a preliminary version. At the end of this process, NIST released Version 1.0 of the "Framework for Improving Critical Infrastructure Cybersecurity" (the Framework) on February 12, 2014.

NIST describes the Framework as providing a "common taxonomy and mechanism for organizations to: 1) Describe their current cybersecurity posture; 2) Describe their target state for cybersecurity; 3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process; 4) Assess progress toward the target state; 5) Communicate among internal and external stakeholders about cybersecurity risk."[4] The Framework, which focuses on risk-management, is technologically neutral and is not industry-specific.[5] It is designed to complement, rather than replace, a company's existing risk-management practices.[6] NIST anticipates that the Framework "will continue to be updated and improved as industry provides feedback on implementation."[7]

The Framework consists of three parts. First, the Framework Core "presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level."[8] Second, the Framework Implementation Tiers "describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework," i.e., they describe general categories of overall cybersecurity sophistication.[9] Third, the Framework Profiles "can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario," i.e., they state an entity's performance (or goals) across the various elements of the Framework Core.[10]

The Framework Core

The Framework Core "presents cybersecurity outcomes identified by industry as helpful in managing cybersecurity risk" and "is not a

checklist of actions to perform."[11] It is presented in the form of a table that effectively explains how, through meeting broadly accepted cybersecurity standards, a critical infrastructure operator can improve its performance of key security functions. The Framework Core is broken into four elements:

- **Functions** "organize basic security activities at their highest level."[12] These functions are: *Identify* ("Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities."); *Protect* ("Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services."); *Detect* ("Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event."); *Respond* ("Develop and implement the appropriate activities to take action regarding a detected cybersecurity event."); and *Recover* ("Develop and implement the appropriate activities to contain the impact of a potential cybersecurity event.").[13]
- **Categories** subdivide functions into "groups of cybersecurity outcomes closely tied to programmatic needs and particular activities." Examples include: "Asset Management," "Access Control," and "Detection Processes."[14]
- **Subcategories** divide categories into "specific outcomes of technical and/or management activities." Examples include: "Data-at-rest is protected," "External information systems are catalogued," and "Notifications from detection systems are investigated."[15]
- **Informative References** are a non-exhaustive list of "specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each subcategory."[16]

The Framework Implementation Tiers

The Framework Implementation Tiers provide entities with a means to categorize their overall cybersecurity performance. However, NIST is careful to explain that "Tiers do not represent maturity levels," and that while "[p]rogression to higher Tiers is encouraged" when such a change is cost-effective and enhances cybersecurity, "[s]uccesful implementation of the Framework is based upon achievement of the outcomes described in the organization's Target Profile(s) and not upon Tier determination."[17]

The four Tiers, each of which is described in terms of "Risk Management Process," "Integrated Risk Management Program," and "External Participation," are:

- **Tier 1: Partial**—Risk management practices are *ad hoc*; there is limited awareness of cybersecurity risk; and participation in external entities (e.g., an Information Sharing and Analysis Center) is limited.
- **Tier 2: Risk Informed**—Risk management practices are approved by management, if not established entity-wide; organizational awareness of cybersecurity risk is not matched by an organization-wide approach for managing that risk; and the entity has not formalized its external interaction capabilities.
- **Tier 3: Repeatable**—Risk management practices are formally approved, expressed as policy, and regularly updated; there is an organization-wide approach to managing cybersecurity risk, including through knowledgeable personnel; and the entity engages in information sharing with external partners.
- **Tier 4: Adaptive**—Risk management practices are updated through a process of continuous improvement; cybersecurity risk management is part of the organizational culture and is based on past activities and continuous system awareness; and the entity actively shares information with partners to

facilitate improved cybersecurity before a cybersecurity event occurs.[18]

The Framework Profile

NIST describes a Framework Profile as "the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization," and explains that a "Profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals."[19] An entity may generate a "Current Profile" and a "Target Profile."[20] In other words, then, a Framework Profile is the assessment that a company generates when it uses the Framework Core to evaluate its cybersecurity posture—e.g., strong in certain categories, weak in others—and to determine which areas it should strengthen in order to manage its cybersecurity risk.

How to Use the Framework

NIST identifies four ways to use the Framework:

- **Basic review of cybersecurity practices**, by comparing an organization's current cybersecurity activities with those outlined in the Framework Core.[21]
- **Establishing or improving a Cybersecurity Program**.
- **Communicating cybersecurity requirements to stakeholders**, including service providers and partners.[22]
- **Identifying opportunities for new or revised informative references**, such as through collaboration with technology leaders and standards bodies.[23]

NIST also includes a subsection entitled "Methodology to protect privacy and civil liberties" in the "How to Use the Framework" section. It responds to the EO's requirement that the Framework include a methodology "to protect individual privacy and civil liberties,"[24] and provides "a general set of considerations and processes" to "address individual privacy and civil liberties implications that may result from cybersecurity operations."[25] The Framework does not identify specific "Informative References" (i.e. existing standards) that an entity might use to protect individual privacy.[26] Instead, it describes general categories of activities for managing risk to individual privacy.[27] Within those categories, it identifies steps the entity might take to protect individual privacy. For example, within the "Awareness and training measures" category, it identifies one steps as: "Applicable information from organization privacy policies is included in cybersecurity workforce training and awareness activities."[28]

Next Steps

Implementation: EO 13636 directs the Secretary of the Department of Homeland Security (DHS) to establish, in coordination with sector-specific agencies, "a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities," including through the establishment of incentives for participation in that program. To that end, DHS launched the "C Cubed" (or "C³") voluntary program[29] to coincide with the release of the Framework. The stated purposes of that program are to: "1) support industry in increasing its cyber resilience; 2) increase awareness and use of the Framework; and 3) encourage organizations to manage cybersecurity as part of an all hazards approach to enterprise risk management."[30] DHS further states that "The C³ Voluntary Program's focus during the first year will be engagement with Sector-Specific Agencies (SSAs) and organizations using the Framework to develop guidance on how to implement the Framework.[31] Later phases of the C³ Voluntary Program will broaden the program's reach to all critical infrastructure and businesses of all sizes that are interested in using the Framework."[32]

Regulation: EO 13636 requires "agencies with responsibility for regulating the security of critical infrastructure" to evaluate "current cybersecurity regulatory requirements" and, "if they are deemed to be insufficient," to propose, within 90 days of publication of the Framework, "prioritized, risk-based, efficient, and coordinated actions … to mitigate cyber risk."[33] EO 13636 similarly recommends that independent regulatory agencies with relevant responsibilities engage in a consultative process "to consider prioritized actions to mitigate cyber risks for critical infrastructure."[34]

Regulatory agencies have not yet indicated what "prioritized actions" they might take in response to the Framework, but at least three categories of action are possible.

First, an agency could attempt to mandate or encourage, either by rule or through guidance, adoption of a portion of the Framework Core.[35]

Second, an agency could impose disclosure requirements based on the Framework. The SEC, for example, recently has pressed registrants for disclosure of cyber risk. It may find the Framework Tiers to provide an appealing template for relevant disclosure requirements.

Third, a regulator could attempt to use the Framework in the exercise of otherwise unrelated enforcement authority. The Consumer Financial Protection Bureau, for example, has authority to bring actions for "abusive acts or practices" against covered financial institutions, and conceivably could seek to prove that, by failing to pursue an appropriate target profile, a company took "unreasonable advantage" of "the reasonable reliance by the consumer on a covered person to act in the interests of the consumer."[36]

Litigation and Insurance: The three elements of the Framework also are likely to play a role in future litigation, as well as in the insurance markets. *First*, the Framework Core provides a vocabulary for identifying a cybersecurity failure (e.g., a failure of detection, identification, etc.), and it specifies particular industry standards that are intended to reduce the risk of such a failure. Though these risk-management tools should properly be expected to reduce, rather than eliminate, risk, and although the framework imposes no mandatory legal obligations, the plaintiffs may attempt to use the failure to meet identified "Informative References" as a basis for liability, whether for a data breach or another form of harm. *Second*, insurance companies may find the Framework Tiers, as well as the more granular elements of the Framework Core, to be useful as they look to build actuarial analyses of cyber risk. *Third*, information relating to a company's work toward a goal Framework Profile may prove to be fertile ground for civil discovery with respect to a company's awareness of cybersecurity risk, as well as its decisions how to prioritize and address those risks.

For more information about the topics raised in this Legal Update, please contact the following lawyers, oryour regular Mayer Brown lawyer.

Howard W. Waltzman
+1 202 263 3848
hwaltzman@mayerbrown.com

Stephen Lilley
+1 202 263 3865
slilley@mayerbrown.com

Endnotes

[1] Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity § 2, 7 (Feb. 12, 2013).

[2] *Id.* § 7.

[3] *Id.*

[4] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (Framework) at 4 (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[5] Framework 4-5. The Framework describes "risk management" as the "ongoing process of identifying, assessing, and responding to risk." It explains: "To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance."

[6] Framework 4.

[7] Framework 2.

[8] Framework 4.

[9] Framework 5.

[10] Framework 5.

[11] Framework 7.

[12] Framework 7.

[13] Framework7.

[14] Framework 8.

[15] Framework 8.

[16] Framework 8.

[17] Framework 9.

[18] Framework 10-11.

[19] Framework 11.

[20] Framework 11.

[21] Framework 13.

[22] Framework 15.

[23] Framework 15.

[24] EO 13636 § 7(b).

[25] Framework 15.

[26] *Cf.* Preliminary Framework App. B, *available at* http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.

[27] Framework 16-17. The categories are governance of cybersecurity risk, approaches to identifying and authorizing individuals to access organizational assets and systems, awareness and training measures, anomalous activity detection and system and assets monitoring, and response activities, including information sharing or other mitigation efforts.

[28] Framework 16.

[29] The full name of the program is the Critical Infrastructure Cyber Community (C3) Voluntary Program.

[30] http://www.dhs.gov/about-critical-infrastructure-cyber-community-c%C2%B3-voluntary-program

[31] EO 13636 § 8(b) requires SSAs to "coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments."

[32] http://www.dhs.gov/about-critical-infrastructure-cyber-community-c%C2%B3-voluntary-program

[33] EO 13636 § 10 (a)-(b).

[34] EO 13696 § 10(e).

[35] The Administration has repeatedly emphasized the voluntary nature of the Framework and the accompanying DHS program. However, the Administration does not control the actions of independent agencies. The Administration's posture also may change if an executive branch agency finds existing regulations insufficient as part of the assessment required by the Executive Order.

[36] *See* 12 U.S.C. § 5531(d).