Client Alert: NIST Releases Draft Updates to Cybersecurity Framework

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 1.19.2017

Recently, the U.S. Department of Commerce, through the National Institute of Standards and Technology (NIST), released a draft Version 1.1 to its Cybersecurity Framework, available here. By their very nature, cybersecurity standards are often vague, difficult to customize to your business, and downright tough to implement, and Version 1.0, released in February 2014, sought to help companies tackle these challenges. Version 1.1 of the Cybersecurity Framework seeks to address frequently asked questions NIST has received since the release of Version 1.0, as well as comments received in response to a December 2015 request for information and a recent public workshop. As with Version 1.0 of the Cybersecurity Framework, use of Version 1.1 is voluntary.

One primary area Version 1.1 seeks to address is supply chain risk management for cybersecurity issues. With more high profile data breaches caused by vendor access and increasing regulatory attention and expectations regarding vendor oversight, cyber supply chain risk management presents challenges to many organizations. Version 1.1 introduces cyber supply chain risk management definitions into each tier, with the lower tiers being organizations that may not fully understand the implications of their cyber supply chain risks or have processes in place to identify, assess, and mitigate those risks, while organizations in tier 4 are those that can quickly account for emerging cyber supply chain risks using real-time or near real-time information. Version 1.1 also recommends communicating and verifying cybersecurity requirements among relevant stakeholders as one aspect of cyber supply chain risk management, which may include:

- Determining cybersecurity requirements for suppliers and IT partners;
- Including contractual terms regarding cybersecurity requirements in supplier agreements;
- Communicating to suppliers how those requirements will be verified and validated;
- Verifying the requirements are met though assessment methodologies, and

- Governance and management of these activities.

Additionally, Version 1.1 provides a new means of measuring an organization's progress in identifying and managing cybersecurity through a comprehensive set of cybersecurity measures and metrics. This new section is dedicated specifically to managing cybersecurity risks with the business's overall objectives; including helping understand the relationship between that organization's business objectives and cybersecurity measures. Understanding this relationship then allows businesses to examine cost effectiveness of various cybersecurity activities.

NIST is seeking public comment to the draft Version 1.1 Cybersecurity Framework, and intends to release a final Version 1.1 in the fall of 2017. Feedback ad comments can be directed to cyberframework@nist.gov.

Many of our clients often question which cybersecurity standards to implement as there are several frameworks to follow. The NIST Cybersecurity Framework, including the additional clarifications provided in draft Version 1.1, provides a helpful starting point for many organizations. As cybersecurity risks continue to evolve, organizations must ensure that they are prepared to manage them. If you have questions about these updates to the framework or other cybersecurity matters, please contact Heather Enlow-Novitsky, Sarah Spector, or your Vorys attorney.