GTC

LAWYERS + STRATEGISTS

NIST CYBERSECURITY FRAMEWORK EXECUTIVE SUMMARY

October 2017

- **NIST Cybersecurity Framework** – v.1.0 published in 2014, draft v 1.1 released Jan. 2017, currently used by approx. 30% of U.S. organizations (per NIST/Gartner).
    - Updated draft (v1.1 released January 2017) emphasizes the importance of managing vendors and supply chain risks and introduces cybersecurity metrics and measurements.
    - Second draft expected to be released in Fall 2017 with a 30-day comment period to follow.
    - Final version expected to be released in 2018.
    - According to the Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure signed by President Trump in May 2017, federal agencies must apply the NIST Cybersecurity Framework to their operations.

- Generally, NIST Framework is not (yet) a legal or regulatory requirement for private businesses.
    - Provides guidance for best practices and collects standards for a wide variety of industries. Not "one size fits all".
    - Outside partners/customers and investors/acquirers may seek a contractual representation and warranty of compliance with the NIST Framework.

- Framework is divided into: 1) the Core, 2) the Implementation Tiers, and 3) the Profile.
    - **Core** includes key cybersecurity functions 1) **identifying** vulnerabilities and key information assets, 2) **protecting** against cyber threats, 3) **detecting** cybersecurity events/breaches, 4) **responding** to breaches, and 5) **recovering** from breaches.
        - Each category is divided into more precise subcategories with specific standards. For example, the "Protect" function has seven categories: Identity Management and Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology. An organization can choose the category of interest such as "Data Security" which divides into eight subcategories. Then, choose the subcategory that fits specific needs, such as "data-in-transit protection," which would include these standards: "CCS CSC, COBIT, ISA, ISO/IEC and NIST SP 800-53 Rev. 4." (See "Core" spreadsheet attached).
    - **Implementation Tiers** provide a grading system for an organization's management of cybersecurity.
        - Tiers range from Partial (Tier 1) to Adaptive (Tier 4 - highest). Not everyone has to be at Tier 4 for all aspects of cybersecurity; a risk/cost analysis is appropriate.
    - **Profile** is an assessment in which an organization identifies its Current Profile (present state) and a Target Profile (desired state).
        - Categories and Subcategories in the Core are used develop the Profiles, with consideration of business drivers and a risk assessment.
        - Goal is to chart a course from the Current Profile to the Target Profile.