NIST Issues Discussion Draft of Preliminary Cybersecurity Framework

2013-08-30

The National Institute of Standards and Technology ("NIST") has posted a discussion draft of the preliminary version of the voluntary federal cybersecurity standards NIST was directed to develop under the executive order on critical infrastructure cybersecurity issued by President Obama in February.[1] A preliminary version of the standards, known as the Cybersecurity Framework, are due by October 10. The discussion draft was made public to encourage comments in advance of NIST's fourth public workshop on the framework, to be held at the University of Texas at Dallas on September 11.

The discussion draft emphasizes a risk-management approach to businesses' cybersecurity efforts. It divides the Framework into three parts: a Core, Implementation Tiers, and a Profile.

The Core in turn consists of five functions, designed to provide high-level structures for organizing cybersecurity activities:

- Identify–Develop the institutional understanding of the organizational systems, assets, data and capabilities that need to be protected; determine priority in light of organizational mission; and establish processes to achieve risk management goals.
- Protect–Develop and implement the appropriate safeguards, prioritized through the organization's risk management process, 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, prioritized through the organization's risk management process (including effective planning), to take action regarding a detected cybersecurity event.
- Recover–Develop and implement the appropriate activities, prioritized through the organization's risk management process, to restore the appropriate capabilities that were impaired through a cybersecurity event.

For each function, the discussion draft identifies existing technical standards, from NIST and

international standards bodies, that may inform carrying out the function.

The Tiers represent ways of gauging increasingly extensive degrees of implementation of the core functions, from partial to risk-informed, to repeatable, to adaptive. A Profile is intended to help organizations "establish a roadmap" for organizational efforts to reduce cybersecurity risks. The discussion draft provides a sample five-step process, including (i) make organization-wide decisions; (ii) establish a target, i.e., desired, profile; (iii) establish a current profile; (iv) compare target and current profiles; (v) implement target profile.

The discussion draft also identifies several specific areas for improvement as the revision of the preliminary Framework moves forward: (i) authentication; (ii) automated indicator sharing; (iii) conformity assessment; (iv) data analytics; (v) international aspects, impacts, and alignment; (vi) privacy; and (vii) supply chains and interdependencies.

---

[1] The preliminary discussion draft is available here. A description of the executive order and the various tasks it assigned to different Executive Branch agencies can be found here.