CARLTON FIELDS

NIST Releases Preliminary Cybersecurity Framework for Critical Infrastructure Organizations

September 05, 2013

In accordance with the President's Executive Order on Cybersecurity, issued earlier this year, the National Institute of Standards and Technology ("NIST") is rapidly preparing a Cybersecurity Framework of best practices and guidelines intended to help organizations, particularly those considered part of the nation's "critical infrastructure," improve their IT and data security. While a full release of the Framework is not expected until October, NIST has released a preliminary draft to seek industry feedback before releasing the Framework for public comment. The preliminary draft is divided into four main sections. The first section is an introduction that provides the Framework's context and rationale. The second section describes the Framework's core functions, which are to identify, protect, detect, respond, and recover. Section two also discusses organizational implementation of the Framework core functions and is intended to help companies in critical infrastructure industries prioritize and manage risk. The third section provides guidance on how to use the Framework to implement and manage an effective data security program. It also provides a five-step example showing how an organization may use the Framework to develop or improve its cybersecurity program. The fourth and last section identifies the following areas of the Framework that need improvement:

- Authentication
- Automated Indicator Sharing
- Conformity Assessment
- Data Analytics
- International Aspects, Impacts, Alignment

- Privacy
- Supply Chains and Interdependencies

Companies operating in the energy sector, finance and banking, health care, transportation, telecommunications, defense, and utilities must know that, while the Framework is considered "voluntary" and intended to supplement, not replace, an organization's cyber risk management process, a non-conforming program will invite added regulatory scrutiny and possibly targeted malicious attacks. A full review of your organization's cyber risk management program, privacy program, and data governance strategy is necessary to assess which areas are in compliance or exceed the standards of the Framework and which need improvement. A public discussion about the Framework is ongoing on Twitter with the hashtag #NISTCSF. Our attorneys provide comprehensive counsel on matters related to information security, privacy, and data breach response.

Authored By

Dennis J. Olle

Related Practices

Business Transactions
Cybersecurity and Privacy