CARLTON FIELDS

NIST Issues Preliminary Cybersecurity Framework for Critical Infrastructure Organizations

October 23, 2013

In accordance with the President's Executive Order on Cybersecurity issued on October 22, 2013, the National Institute of Standards and Technology ("NIST") released the draft of its Cybersecurity Framework, intended to help organizations, particularly those considered part of the nation's "critical infrastructure," improve their IT and data security programs and policies. NIST will open a 45-day public comment period on the preliminary framework and plans to release the official framework in February 2014. The NIST Cybersecurity Framework outlines steps that can be customized to various sectors and adapted by large and small organizations while providing a consistent approach to cybersecurity across industries. It is intended to provide a common "language" and platform for organizations to determine and describe their cybersecurity posture as well as evaluate risk and develop a strategy to address gaps and identify weaknesses. The Framework aims to foster collaboration and communication between governmental and non-governmental actors to improve transparency and mutual accountability in order to strengthen cybersecurity protections at all levels. While the Framework creates some standards and suggests using consistent methodology, it provides sufficient flexibility to allow stakeholders to develop an approach to strengthening cybersecurity that is specifically tailored to their industry and regulatory requirements. Companies and organizations that are considered "critical infrastructure" – those that operate in the energy sector, finance and banking, healthcare, transportation, telecommunications, defense, and utilities – need to be aware that the Framework is intended to supplement their organization's cyber risk management process instead of replace it, but having a non-conforming program will be an invitation for added scrutiny by regulators and possible targeting by malicious attackers. A full review of your organization's cyber risk management program, privacy program and data governance strategy is necessary to assess what areas are in compliance with the NIST Framework and what areas need improvement and strengthening. The NIST Cybersecurity Framework can be

found at http://www.nist.gov/itl/cyberframework.cfm and an announcement of the opening of the official comment period will run in the Federal Register.

Related Practices

Cybersecurity and Privacy
Telecommunications

Related Industries

Telecommunications