wiley

ALERT

NIST Releases Preliminary Cybersecurity Framework for Public Comment

October 22, 2013

Today, the National Institute of Standards and Technology (NIST) released the Preliminary Cybersecurity Framework, a set of standards and practices designed to assist organizations that are responsible for critical infrastructure as they address and manage cybersecurity risk. The government shutdown delayed the Preliminary Framework from its scheduled October 10, 2013, release.

The Preliminary Framework is one of many deliverables put in motion by Executive Order 13636, which directs NIST to develop "a prioritized, flexible, repeatable, performance-based, and cost-effective approach" that will "align policy, business, and technological approaches to address cyber risks."

The Preliminary Framework was the subject of public participation over the spring and summer, including at several workshops held by NIST around the country. The Preliminary Framework precedes NIST's adoption of a Final Cybersecurity Framework. The Final Framework, due in February 2014, will be shaped by comments received by NIST.

The adoption of the cyber standards and practices that will be included in the Final Framework is intended to be voluntary, though the Executive Order mandates that the Department of Homeland Security (DHS) create a Voluntary Program with incentives to encourage companies to adopt the Final Framework. The federal government hopes that its Final Framework will spur improvements to cybersecurity practices throughout industry and not just in critical infrastructure sectors.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Nova J. Daly
Senior Public Policy Advisor
202.719.3282
ndaly@wiley.law

Henry Gola
Partner
202.719.7561
hgola@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

Telecom, Media & Technology

A great deal of uncertainty surrounds the content and structure of both the Final Framework and the Voluntary Program. Industry groups are concerned that the standards recommended by NIST could become de facto obligations or be made mandatory by regulatory agencies that have been instructed in the Executive Order to evaluate the adequacy of existing regulations and consider new obligations to mitigate cyber risks to critical infrastructure.

Industry comments on the Preliminary Framework are due **45 days** after publication of the Preliminary Framework in the *Federal Register*.