WINSTON & STRAWN LLP

BLOG

# Commerce Department Releases Cybersecurity Framework

FEBRUARY 14, 2014

A set of voluntary, risk-based industry standards and best practices aimed at helping private financial, health care, energy and other companies manage cybersecurity risks and targeted toward improving national and economic security was released this week by the Commerce Department's National Institute of Standards and Technology (NIST) pursuant to Executive Order 13636 issued by President Barack Obama in 2013. The report – *Framework for Improving Critical Infrastructure Cybersecurity* – was a collaborative effort between the government and the private sector and recommends a wide range of best practices targeted toward reducing and better managing cybersecurity risks for companies whose systems and assets, whether physical or virtual, are vital to the United States. The framework is meant to provide a consistent approach for managing cybersecurity risks by helping companies identify their current cybersecurity levels, determine whether those levels are in in line with their current business structure, and establish goals to maintain an appropriate level of cybersecurity. Companies' implementation is expected to vary according to their individual risks and to maximize the impact of each dollar spent. The NIST touted the voluntary framework as "the next step to improve the cybersecurity of our Nation's critical infrastructure." In issuing the report, the NIST noted that cybersecurity threats increasingly "exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk." Cybersecurity risk also "affects a company's bottom line" by driving up costs, impacting revenue and harming a company's ability to innovate and maintain a loyal customer base, according to the report. Key industry concerns considered in drafting the report were the cost-effectiveness of cybersecurity risk measures and the importance of avoiding undue regulatory requirements on businesses. The NIST plans to update the report as industry provides feedback on implementation of the new standards. The report also recommended companies pay close attention to the privacy and civil liberties implications that may arise when personal information is used, collected, processed, maintained, or disclosed in connection with an organization's cybersecurity activities. While the report contained recommended actions including the incorporation of privacy principles like data minimization, some experts have expressed concern that the privacy provisions are weaker than they were in earlier drafts. Other criticism centered on the voluntary nature of the framework. Executive Order 13636 by President Obama called for the development of a voluntary Cybersecurity Framework that provides a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" to manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services. It also required that any proposed framework include a methodology to protect privacy and civil liberties within cybersecurity programs.

**Tip: Regardless of whether a business might be viewed as "vital to the nation's critical infrastructure" by the NIST or others, all companies would be well served to consider and review the industry standards and best practices cited in the NIST report. While the framework is voluntary and applies only to certain industries, courts and regulators around the country may look to these standards as a baseline for determining whether companies, in any industry, adequately protected their data.**

2 Min Read

## Author

Steven Grimes

## Related Locations

Chicago

## Related Topics

Data Breach

## Related Capabilities

Privacy & Data Security

Health Care

# Related Professionals

Steven Grimes

*This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.*