wiley

ALERT

NIST's Final Cybersecurity Framework Will Drive Oversight and Enforcement

February 13, 2014

On February 12, the Obama Administration released the National Institute of Standards and Technology's (NIST) Final Cybersecurity Framework, as directed by the President's February 2013 Executive Order and Presidential Policy Directive. The Framework sets forth voluntary cybersecurity guidelines for Critical Infrastructure entities, and will be the centerpiece of a Voluntary Program run by the Department of Homeland Security (DHS) and various sector-specific agencies. Release of the Framework triggers a 90-day review process by federal agencies to evaluate existing authorities and provision. Beyond regulatory review, the Framework is likely to influence federal enforcement efforts in data and cybersecurity. Given near-daily news of breaches and intrusions, the Federal Trade Commission's (FTC) aggressive enforcement posture, and the possibility of legislation or regulation, businesses should follow the implementation of the Framework, and the Voluntary Program, as they will drive cybersecurity expectations in the future.

NIST Releases Final Cybersecurity Framework. NIST released the Final Cybersecurity Framework, a voluntary set of standards and practices designed to manage cybersecurity risk for organizations responsible for critical infrastructure. In tandem with the Framework's release, DHS unveiled aspects of the Voluntary Program, including the Critical Infrastructure Cyber Community (C^3) Program, which is designed to support use of the Framework, particularly by small and mid-sized companies. The Framework and the Voluntary Program are cornerstones of Executive Order 13636, which the President issued to spur improvements to cybersecurity practices throughout industry.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Henry Gola
Partner
202.719.7561
hgola@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Government Contracts

Privacy, Cyber & Data Governance

Telecom, Media & Technology

The Final Framework makes some tangible changes from the Preliminary Framework released in October, on which NIST received more than 200 comments. Notably, it removes a separate appendix for privacy controls and instead incorporates an alternative methodology preferred by industry. The alternative methodology makes clear that its guidance is limited to privacy and civil liberties issues resulting from an organization's cybersecurity operations. In addition, the Final Framework clarifies what it considers "successful implementation," stating that it "is based upon achievement of the outcomes described in the organization's Target Profile(s) and not upon Tier Implementation."

The release of the Framework shifts focus to DHS, which the Executive Order directs to create a Voluntary Program with incentives to encourage companies to adopt the Final Framework. According to DHS, the C^3 Voluntary Program will focus on supporting industry's understanding and use of the Framework, including through outreach efforts. The Program will encourage industry feedback, and DHS indicates that future Requests for Information will "create opportunities for the general public to provide input on cybersecurity solutions and policies."

The Framework Is Likely to Shape Future Regulation and Enforcement. The Framework is likely to impact private security efforts—from risk assessment to enforcement activities—far beyond Critical Infrastructure owners and operators that may participate in the Voluntary Program. Federal agencies must, under the Executive Order, report to the President on their authorities and options, and state regulators are assessing action on cybersecurity. But whatever happens with legislation or regulation, companies and regulators may look to the Framework to inform case-by-case enforcement.

The most notable enforcement threat is from the FTC. The FTC has been active on data security, bringing and settling 50 enforcement actions against businesses that the FTC believed misled consumers about the companies' use of reasonable or adequate security measures and failed to protect information adequately from electronic security threats. These settlements often result in obligations to improve data security, clarify expectations, and obtain periodic third-party assessments of security programs for 20 years.

A major test of FTC authority reveals the potential importance of the Final Framework. Wyndham Hotels has challenged the FTC's authority in a lawsuit over the company's data security practices. Between 2008 and 2010, cyber criminals hacked into the computer networks of Wyndham Hotels & Resorts and Wyndham-branded hotel franchises, stealing customers' payment card data from Wyndham franchises. The FTC sued, claiming that Wyndham engaged in deceptive and unfair practices—that it did not abide by the privacy policy it disseminated to its customers, and that it failed to use "reasonable and appropriate" safeguards to protect personal information on its systems. Wyndham challenged the FTC's authority to punish companies' cybersecurity breaches as "unfair practices," and argued that because there are no binding regulations governing its data security obligations, there was no adequate notice of specific substantive expectations Wyndham can been said to have violated. The parties and the court have looked to NIST's emerging Cybersecurity Framework as an example of the sort of government action that might provide adequate guidance on what is "reasonable." But it is not clear that the Final Framework provides adequately specific guidance, or any sort of safe harbor for organizations that seek to implement it.

Despite the uncertainty facing businesses over the adequacy of their security practices, the FTC is not backing away from post-breach enforcement. The FTC issued an order in a case against *LabMD* on January 16, 2014, explicitly interpreting Section 5 to extend to data security. And, FTC Chairwoman Edith Ramirez testified before two congressional committees earlier this month, touting the FTC's data security enforcement record. Companies should expect continued government interest in cybersecurity, whether through regulation and agency oversight or—in the absence of legislation or regulation—reliance on post-hoc enforcement action.

Conclusion. Though the government and private sector still have work to do on the Framework, the Voluntary Program, and possible regulation and legislation, the Wyndham case makes clear that the private sector should pay attention now. The implementation of the Framework—depending on how it is deployed—could influence on how courts, legislators, and regulators evaluate cybersecurity practices going forward.