Client Alert

November 2013

NIST Issues Preliminary Cybersecurity Framework

On October 29, 2013, the National Institute of Standards and Technology (NIST) published its Preliminary Cybersecurity Framework (Preliminary Framework) in the Federal Register. Issued pursuant to the President's February 2013 Executive Order on Improving Critical Infrastructure Cybersecurity, the Preliminary Framework includes standards, procedures and processes to reduce cyber risks. NIST is seeking written comment on the Preliminary Framework by December 13, and is expected to publish a final version in February 2014. As discussed below, although it is a voluntary, nonregulatory protocol, the Framework will likely become a benchmark against which companies' cybersecurity practices are compared.

The Preliminary Framework is organized into five broad functions: Identify, Protect, Detect, Respond and Recover. Each function has multiple categories, which are more closely tied to programmatic activities. They include activities such as "Asset Management," "Access Control" and "Detection Processes." The categories, in turn, have subcategories that support technical implementation. Examples of subcategories include "Asset vulnerabilities are identified and documented" and "Organizational information security policy is established." Finally, the Framework includes Informative References, which specify sections of existing standards and practices that are common among various critical infrastructure sectors and illustrate methods to accomplish the activities described in each subcategory.

The Preliminary Framework gives companies discretion on how to prioritize different aspects of network security, what level of security to adopt and which standards, if any, to draw from. It does not include mandates to adopt a particular standard or practice. However, the Executive Order directs regulatory agencies to determine if their current cybersecurity regulations are sufficient in light of the Preliminary Framework, and to take regulatory action within 90 days of the publication of the final Framework in February 2014. This could lead to revised cybersecurity regulations.

In addition, the administration has stated that it will use incentives and market forces to advance the goals of the Framework. Pursuant to the Executive Order, the Department of Homeland Security is establishing a voluntary program to support widespread adoption of the Framework. In connection with that program, the administration is evaluating eight different types of incentives that could be used to encourage adoption of the Framework. As described by the White House, the eight areas of incentives are:

- Cybersecurity insurance — working with industry to build underwriting practices that promote adoption of Framework standards, and fostering the development of a competitive insurance market;
- Federal grants conditioned on adoption of the Framework;
- Process preferences — establishing adoption of the Framework as a criteria for prioritizing who receives technical government services in nonemergency situations;
- Liability limitations (would require congressional action) — reduced liability for entities that adopt the Framework and participate in the voluntary program, including, for example, reduced tort liability, limited indemnity, lower burdens of proof or a federal legal privilege that preempts state disclosure requirements;

- Streamlined regulations — ensuring that the Framework interacts in an effective manner with existing regulatory structures, eliminating overlaps among existing regulations and reducing audit burdens;
- Public recognition for participants in the voluntary program;
- Rate recovery for price-regulated industries — allowing utilities to recover for cybersecurity investments related to adoption of the Framework and participation in the voluntary program; and
- Cybersecurity research in areas where commercial solutions are not currently available.

Various sector-specific agencies are reviewing these incentives to determine which, if any, would be appropriate for their respective sectors, and inviting industry input as part of that review. Companies may be well served by some of these incentives if they are incorporated into the government's program to encourage adoption of the Framework.

As a result of the incentives, the voluntary program and the cybersecurity regulatory review, the Framework may significantly influence underwriting standards and create a general benchmark against which companies' cybersecurity practices are judged in the event that they become the subject of litigation. Companies may wish to engage in the policy and regulatory process in order to influence the content of the Framework, the possible follow-on revision to existing cybersecurity regulations, and the decision to use incentives to encourage adoption of the Framework.

Companies also should consider measuring their own practices against the Framework by assessing and updating their corporate governance structure, policies, procedures and regulatory compliance systems for information security, as well as reviewing and updating internal response plans and procedures for addressing cyber incidents. Part of that review should include consideration of private-private and public-private information sharing programs that are designed to provide industry information security professionals with current cybersecurity threat information. It should also include an evaluation of available financial protection, including an analysis of vendor agreements and insurance programs. Companies may consider obtaining specialized insurance products designed to protect against cybersecurity risks. With a number of very different insurance products of that type on the market, however, companies need to study their own cyber risks and existing insurance in order to obtain appropriate protection.

Lisa J. Sotto
lsotto@hunton.com

Lawrence J. Bracken II
lbracken@hunton.com

Paul M. Tiao
ptiao@hunton.com

John J. Delionado
jdelionado@hunton.com

Lon A. Berk
lberk@hunton.com

Neil K. Gilman
ngilman@hunton.com

Frederick R. Eames
feames@hunton.com

Michael A. Oakes
moakes@hunton,com

Mark W. Menezes
mmenezes@hunton.com

Aaron P. Simpson
asimpson@hunton.com

Walter J. Andrews
wandrews@hunton.com

William T. Um
wum@hunton.com