VENABLE® LLP

Cybersecurity Alert

November 2013

NIST Holds Fifth Workshop on Cybersecurity Framework; Incentives Still Lacking

AUTHORS

Michael J. Baader
Jamie Barnett, Rear Admiral (Ret.)
Dismas Locaria
Anthony J. Rosso
Brian M. Zimmet
Jason R. Wool

RELATED PRACTICES

Homeland Security

RELATED INDUSTRIES

Cybersecurity

ARCHIVES

2013 2009 2005
2012 2008 2004
2011 2007 2003
2010 2006

On November 14-15, 2013, the National Institute of Standards and Technology (NIST) held a **workshop** at North Carolina State University on the **preliminary Cybersecurity Framework** (PCF). Venable attended the workshop in Raleigh, as well as all of the previous NIST workshops addressing the Framework.

NIST does not plan to revise the PCF until the release of the final Cybersecurity Framework in February of 2014, per **Executive Order 13636**. However, NIST held the previously unplanned fifth workshop in order to address widespread industry concerns regarding adoption (including incentives) and implementation of the Framework, as well as the controversial privacy appendix attached to the PCF as Appendix B, among other topics. Moreover, interested parties still have several weeks to provide comments on the PCF before the completion of a 45-day **request for comments**, which NIST issued on October 29, 2013.

Overview

The fifth workshop followed the same template as previous meetings, combining panel discussions with topic-specific working sessions. The first day's panels included a discussion of privacy and civil liberties issues raised by the PCF as well as a question and answer session featuring NIST representatives that was led by Matt Eggers of the U.S. Chamber of Commerce. The panels were followed by breakout sessions on the following topics:

- Small and Medium Business Considerations;
- How to Use the Framework;
- Voluntary Critical Infrastructure Cybersecurity Program;
- Research and Development;
- Framework Ecosystem Development; and
- Privacy and Civil Liberties.

Current Lack of Incentives

With no public movement expected on the Framework itself until the final version is released in February 2014, much of industry's attention has turned to the voluntary program led by DHS intended to spur adoption of the Cybersecurity Framework by owners and operators of critical infrastructure. The EO directs DHS to "coordinate the establishment of a set of incentives designed to promote participation in the [voluntary program,]" however the vast majority of these incentives would likely require legislation to be realized.

As a result, DHS stated at one of the topic-specific working sessions that it can only offer "a very limited set of incentives" in the near term. Indeed, it appears that the only incentive mentioned by DHS that would be available at "launch time" in February is prioritization of support and technical assistance. Other "incentives" noted in the DHS presentation include continuing engagement with the insurance industry and private sector "to understand the role of insurance in organizational risk," coordinating with the General Services Administration and the Department of Defense on procurement considerations, working to link existing federal grant programs to adoption of the Framework, discussing rate recovery for price-regulated industries with responsible state and federal agencies, and examining the potential for regulatory streamlining to promote adoption.

Presumably the lack of meaningful incentives at this stage is a result of the poor prospects for any legislation in the U.S. Congress for the remainder of 2013. As a result, NIST representatives appealed to the business community to adopt the Framework in order to allow organic markets – and market-driven

incentives – to form around it instead of insisting on Government-sponsored incentives to encourage adoption. A DHS representative also appealed to the business community to view the voluntary program as a partnership with government and to participate in it because the real benefits of the program will come from utilization and because the greater cybersecurity of the nation is the biggest incentive.

A number of audience members nonetheless emphasized the need for Government-sponsored incentives in order to justify participating in the voluntary program from a business perspective.

Liability Concerns

Attendees were also vocal about the potentially increased exposure to liability they will face as a direct result of the Framework. "The fact of the matter is," said one audience member at the DHS presentation, "we might all sing 'Kumbaya' here, but there are people out there who might want to sue us, and the Framework does raise a new issue related to standard of care."

Although it has not yet been proposed as an incentive by DHS, the SAFETY Act, as an existing liability management tool, is well-suited to address certain industry concerns regarding liability. More importantly, protection under the SAFETY Act could attract significant interest in adopting the Framework as an initial matter, while Congress and various markets develop other attractive incentives.

The release of the PCF provides owners and operators of critical infrastructure with a better understanding of the likely contents of the final Cybersecurity Framework. As the release date of the final version approaches, currently scheduled on February 12, 2014, questions regarding the liability implications associated with adoption or non-adoption of the Framework are more important than ever.

Venable addressed some of these questions in its recent **live presentation and webinar**, *Cyber Sticks and Carrots: How the NIST Cybersecurity Framework, Incentives, and the SAFETY Act Affect You*, on September 25, 2013.

We encourage owners and operators to contact us with questions regarding cyber liability and risk management, including issues relating to insurance, the SAFETY Act, and corporate governance.

Venable will continue to closely follow NIST's finalization of the Cybersecurity Framework, as well as DHS' development of the voluntary program. Venable's attorneys are well-positioned to answer any and all questions regarding the Cybersecurity Framework, having participated in and attended all relevant meetings conducted by NIST since the Executive Order was released in February.

* * * * *

Venable LLP offers a broad array of legal services to a variety of different players within the cybersecurity arena. Our attorneys are adept at understanding complex client issues and tapping into the extensive experience of our many practice areas including privacy and data security, e-commerce, intellectual property, government contracting, telecommunications, energy, and corporate.

If you have any questions concerning this alert, please contact any of the authors.