VENABLE® LLP

Cybersecurity Alert

September 2013

NIST Holds Fourth Workshop on Cybersecurity Framework

AUTHORS

Michael J. Baader

Jamie Barnett, Rear Admiral (Ret.)

Dismas Locaria

Anthony J. Rosso

Brian M. Zimmet

Keir X. Bancroft

Jason R. Wool

RELATED INDUSTRIES

Cybersecurity

ARCHIVES

2013
2012
2011
2010
2009
2008
2007
2006
2005
2004
2003

On September 11-13, 2013, the National Institute of Standards and Technology (NIST) held its fourth and – for now – final workshop on the preliminary Cybersecurity Framework. The Framework is being developed pursuant to President Obama's February **Executive Order** (EO) on critical infrastructure cybersecurity. NIST released a **draft** of the preliminary Framework **prior to the workshop**.

Because much of the drafting of the preliminary Framework had been completed, discussion largely focused on how to promote executive engagement on issues relating to cybersecurity, implementation of the Framework, and what participation in the Department of Homeland Security (DHS) voluntary program would look like. Officials also attempted to address head-on the widespread concern that the Framework would be used to impose additional regulation on the 16 critical infrastructure sectors.

Venable has attended all of NIST's workshops on the Framework and will host a **live presentation and webinar**, *Cyber Sticks and Carrots: How the NIST Cybersecurity Framework, Incentives, and the SAFETY Act Affect You*, on September 25, 2013. Former Deputy Secretary of Homeland Security Jane Holl Lute will give the keynote speech.

Significance of Critical Infrastructure Again Emphasized

Dr. Patrick Gallagher, acting Deputy Secretary of Commerce and Director of NIST, kicked off the workshop by reiterating the relationship of cybersecurity to national security. Recalling the events of September 11, 2001 – exactly 12 years prior to the date of the conference – Gallagher re-emphasized the central mission of the EO and the Cybersecurity Framework, *i.e.* the protection of our nation's most critical infrastructure, which, he noted, is defined in the EO as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." A number of panelists also alluded to this core mission, particularly with regard to industrial control systems, which affect "tangible assets" and can even affect personal safety.

Cyber-Risk as Business Risk

NIST representatives emphasized that the message for senior executives at firms that own or operate critical infrastructure is that cyber-risk must be understood as, and managed like, any other form of corporate risk. They noted that senior executives must understand that decisions concerning cyber-risk management will affect their corporations in the marketplace, in terms of maintaining and growing customer base, reducing costs, increasing revenue, protecting corporate reputation, and more. Similarly, stakeholders repeatedly stated that, in order to promote adoption of the Cybersecurity Framework, NIST must sell the concept of cyber-risk management – not the Framework itself.

Implementation

Many participants expressed concern that the draft preliminary Framework lacks specific guidance with regard to implementation and requested that NIST issue further instructions for potential adopters regarding how to use the Framework. Others worried that the process of mapping existing cybersecurity practices to the categories and sub-categories set forth in the draft would be onerous. With these concerns in mind, a number of stakeholders recommended that the sector-specific agencies responsible for the 16 critical infrastructure sectors be tasked with providing guidance and advice on implementation of the Framework specific to each sector and/or sub-sector. Some participants even suggested that each sector should have its own specific maturity model instead of the standardized tier/profile system utilized in the draft preliminary Framework.

Concerns About Regulation

Stakeholders repeatedly voiced concern that the Framework, though nominally voluntary, would be used to increase the regulation of critical infrastructure. In response to these concerns, which have been voiced throughout the NIST stakeholder process, Andy Ozment of the National Security Staff spoke about the Administration's commitment to a voluntary approach to increasing the cybersecurity of Critical Infrastructure as a "preferred path." However, he also implied that continued reliance on a voluntary approach would depend on the quality of the Framework crafted by the NIST stakeholders as well as the level of adoption of the Framework following its finalization.

"The Administration is not pushing for new regulations...[but in those sectors that are already regulated,] those regulatory agencies have an existing mandate to protect the public and therefore they will necessarily consider the role of the framework in addressing that responsibility, and the EO specifically calls on regulators to look at the framework when they are considering that responsibility." The latter statement appears to be a reference to section 10 of the EO. Further, Ozment stated that the administration has "consistently supported the full range of executive and legislative actions that we need to protect our critical infrastructure" and that "voluntary success here could reduce the drive towards greater regulation elsewhere."

Publication and Next Steps

The preliminary Cybersecurity Framework will be issued on October 10, 2013, and will be subject to a 45-day public comment period. NIST has stated that it will hold additional workshops in the future concerning the Framework, but it has not provided any specifics at this time.

Venable Webinar

The upcoming webinar will take place on September 25, 2013, and will provide a holistic overview of the currently known information on the Framework and the voluntary program to adopt it that will be established by DHS. In addition to featuring a keynote speech from Secretary Lute, the President and CEO of the Council on Cybersecurity and former Deputy Secretary of DHS, the webinar will also feature presentations by Venable's own cybersecurity practitioners, who will provide key insights and industry updates.

The webinar will also include a review of the potential incentives for adoption of the Framework and the currently available protections available under the SAFETY Act, which can be utilized in conjunction with the Framework or another set of cybersecurity standards or guidelines to substantially reduce liability arising from acts of terror. **Registration is still open for the event**.

Venable will continue to closely follow NIST's progress on the development of the Cybersecurity Framework, including the issuance of the preliminary Framework for public comment. With the publication of the preliminary Framework due in less than a month, readers may have questions regarding the impact that the Cybersecurity Framework will have on their respective businesses. Venable's attorneys are well-positioned to answer any such questions, 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.