VENABLE® LLP

Cybersecurity Alert

April 9, 2013

NIST Holds First Workshop on Executive Order Cybersecurity Framework

AUTHORS

Michael J. Baader

Jamie Barnett, Rear Admiral (Ret.)

Dismas Locaria

Anthony J. Rosso

Brian M. Zimmet

Jason R. Wool

Sejal C. Shah

RELATED PRACTICES

Communications

Government Contracts

Energy

RELATED INDUSTRIES

Cybersecurity

Government Contractors

ARCHIVES

2013
2012
2011
2010
2009
2008
2007
2006
2005
2004
2003

On April 3, 2013, the National Institute of Standards and Technology (NIST) held a workshop at the Department of Commerce in which it offered a sneak preview of the Cybersecurity Framework required under the recently-issued **Executive Order on critical infrastructure cybersecurity**. The Workshop, held five days prior to the comment deadline for NIST's recently-issued **Request for Information** (RFI) on the Cybersecurity Framework, consisted of five panel discussions as well as several additional speakers and covered many of the varying considerations and perspectives that will play a role in the development of the Framework. This day-long event included detailed discussion of a number of issues related to the implementation of February's Cyber Executive Order (E.O. 13636).

In addition, NIST has issued a **Notice of Inquiry** (NOI) to determine incentives that would increase adoption of the Cybersecurity Framework. Venable attorneys will be working with critical infrastructure owners and operators to prepare comments responding to the NOI by the April 29, 2013 deadline and seeks your input.

Highlights of the April 3rd workshop are summarized below.

Announcement of Additional Industry Workshops

One of the most notable pieces of information from the workshop was the announcement that there would be three more industry workshops, which would be more in-depth and would involve far greater participation of attendees. The first of these workshops will be held at Carnegie-Mellon University in Pittsburgh, PA on May 29 – 31. The other two workshops will tentatively be held during the weeks of July 15 and September 9, with locations yet to be announced. The May 29 – 31 workshop will focus in particular on risk management, cyber hygiene, and tools & metrics. Before the first industry workshop, NIST will make public its initial analysis of responses to the RFI and use the commenters' input as a starting point for more in-depth discussions.

DHS's Thoughts on Performance Goals

Another highlight of the workshop involved Bruce McConnell, Senior Counsel (Cyber) to National Protection and Programs Directorate at the Department of Homeland Security (DHS), explaining DHS's preliminary thoughts on the performance goals that the Secretary of DHS must provide for the Cybersecurity Framework. E.O. 13636, Sec. 7(d). The Executive Order requires the Secretary to provide performance goals that are informed by DHS' identification of Critical Infrastructure at greatest risk. In previous discussions of the Executive Order, speakers from NIST and DHS have stated that achievement of the performance goals would be the overall metric of "success" for entities that participate in the voluntary program to implement the Cybersecurity Framework.

McConnell stated that the thinking on performance goals is that adoption of the Framework will give the entity a **high** level of confidence that the **essential services** it provides will continue to be delivered to its **critical customers** in the face of **most** cyber incidents **directly affecting** the entity. McConnell stressed, however, that the working performance goals contain numerous terms – the bold terms in the previous sentence – that will require further explanation and interpretation, and he suggested that stakeholders will have an opportunity to participate in this process.

Discussion Regarding the Cybersecurity Framework

In light of many statements made at the workshop as well as at previous events featuring NIST and DHS speakers, several consensus topics have become apparent, making their inclusion in the Cybersecurity Framework likely. These consensus topics include risk assessment and management, metrics, and basic cyber hygiene. In addition, many speakers agreed that the Framework must be scalable, prioritized, not overly complex, market driven, automatable and should not conflict with other government-issued cybersecurity frameworks or laws, as many companies have a global presence or may be otherwise regulated, as in the case of the electric industry in the United States. There was also broad agreement that "check the box" does not work, especially in a business environment, and that a risk-based, outcome-focused approach is necessary.

Many panelists spoke of the need to balance IT security with standard business concerns/obligations. The question of whether to spend on cybersecurity or other business needs – and, if the former, where to draw the line as to what constitutes a sufficient security investment – was consistently repeated by the panelists. Although this question is connected to risk assessment and management, as well as to the development and implementation of a meaningful set of metrics, a number of speakers hinted that this may be an area where the Framework could add meaningful value to those entities that adopt it.

Many speakers agreed that a roadmap or paradigm-framing document was necessary before stakeholders begin work on the substantive details of the Cybersecurity Framework. Per Scott Saunders of Sacramento Municipal Utility District, this includes answering the question, "what are we protecting and what are the threats?"

As readers familiar with the Cybersecurity Framework RFI know, NIST is particularly interested in "the applicability of existing publications to address cybersecurity needs" in developing the Framework. On this topic, Patrick Gallagher, Director of NIST and Under Secretary of Commerce for Standards and Technology, stated that the Cybersecurity Framework will probably include a collection of references to existing standards. Although it is likely that many standards and guidelines will be referenced in the RFI comments, existing publications that received repeated mention by speakers at the workshop included the **Critical Infrastructure Protection (CIP) Standards** currently enforced by the Federal Energy Regulatory Commission; the **20 Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines**; NIST's **SP800-53, SP800-30, and SP800-39**; ISACA's **COBIT 5** IT governance framework; and the **ISO 27000 series**.

Incentives

Finally, with regard to incentives, there was widespread agreement among the panelists that liability protection will be necessary to obtain widespread adoption of the Cybersecurity Framework, although it was also acknowledged that legislation will likely be necessary to provide this incentive. At previous events on the Executive Order, speakers (including Secretary Napolitano of DHS) have also mentioned procurement preferences as well as a government-backed "seal of approval" for entities that adopt the Framework as part of the voluntary cybersecurity program required under the Executive Order. In order to better determine what incentives would increase adoption of the Cybersecurity Framework, NIST also issued the **NOI** on March 28, 2013 to "develop a clearer picture of existing and potential incentives."

As mentioned, Venable attorneys will be working with critical infrastructure owners and operators (including companies in the energy, telecommunications, and banking sectors, to name a few) to prepare comments responding to the NOI by its deadline of April 29, 2013. Venable will be actively monitoring and attending workshops and meetings associated with the Cybersecurity Framework over the next several months.

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 listed in the left rail.