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	2009	2005
2012	2008	2004
2011	2007	2003
2010	2006	

Cybersecurity Alert

September 2013

NIST Releases Draft Preliminary Cybersecurity Framework in Advance of Dallas Workshop

On August 28, 2013, the National Institute of Standards and Technology (NIST) released the **first publically available draft** of the preliminary Cybersecurity Framework, which is being developed at the direction of President Obama's February **Executive Order** on critical infrastructure cybersecurity. The Executive Order requires NIST to issue a preliminary draft of the Framework by October 10, 2013.

In anticipation of that deadline, and to give stakeholders an opportunity to participate in the revision of the draft, NIST will host a fourth and final workshop on September 11-13, 2013 at the University of Texas at Dallas before issuing the preliminary Cybersecurity Framework for public comment.

Venable has attended all of NIST's workshops on the Framework and will be in attendance in Dallas to continue providing coverage on the Framework development process to its clients.

In addition, Venable 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.

Overview of Draft Framework

The draft preliminary Framework largely reflects the characteristics originally set forth in the **Draft Outline of the Framework** released prior to NIST's **July 10-12 workshop** in San Diego. Specifically, the draft retains the outline's proposed structure, consisting of five "core functions" – Know, Prevent, Detect, Respond, and Recover – each of which is divided into categories and subcategories.

At the subcategory level, specific tasks are enumerated alongside selected suggestions for achieving those tasks using existing cybersecurity standards, *i.e.* so-called "Informative References." The listed Informative References, which include well-known standards such as ISA 99, COBIT, the ISO/IEC 27000 series, and NIST's own SP 800-53, are not exhaustive, and entities "are free to implement other standards, guidelines, and practices."

Framework Implementation Tiers and Profiles

One notable change from the draft outline is the replacement of the maturity indicators known as Framework Implementation Levels with Framework Implementation Tiers. The Tiers still reflect an implementing organization's respective maturity under the Framework, measured from zero to four for each core function. Whereas the Framework Implementation Levels were proposed to define specific levels of maturity for each category and subcategory for various roles in an organization, the Framework Implementation Tiers are defined generally and are not role specific, greatly simplifying the measurement of an organization's implementation of the Framework.

A new feature of the draft preliminary Framework is the introduction of Framework Profiles, which make use of the simplified maturity measurement facilitated by the Framework Implementation Tiers. The draft instructs adopting organizations to calculate both their current Profile – consisting of the Tier ratings for each of the core functions – as well as their target Profile, *i.e.* the set of Framework Implementation Tiers that an organization determines it should have based on its assessment of its own cyber-risk. In addition to assisting entities to achieve the right level of risk mitigation by identifying gaps, the Framework Profile concept is intended to assist entities in communicating with one another about cyber-risk.

Areas of Improvement

In addition to providing further detail on the contents of the Cybersecurity Framework, the draft also describes several "areas for improvement" for which "[c]ollaboration and cooperation must increase...to further understanding and/or the development of new or revised standards." The initially identified areas are as follows:

- Authentication;
- Automated indicator sharing;
- Conformity assessment;
- Data analytics;
- International aspects, impacts, and alignment;
- Privacy; and
- Supply chains and interdependencies.

Venable Webinar

The upcoming webinar will take place shortly after the conclusion of NIST's final workshop 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 the Department of Homeland Security (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 following questions will be addressed:

- What has happened since the Executive Order?
- How will the Cybersecurity Framework affect you?
- What is ahead in regulatory and voluntary measures?
- What steps can you take now?

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 remaining workshop and issuance of the preliminary Framework for public comment. With just one workshop remaining before the preliminary Cybersecurity Framework is released for public comment, 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.