VENABLE LLP

Cybersecurity Alert

October 2013

NIST Releases Preliminary 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 2009 2005
2012 2008 2004
2011 2007 2003
2010 2006

On October 22, 2013, the National Institute of Standards and Technology (NIST) **released** the **preliminary Cybersecurity Framework** (PCF) in accordance with section 7(e) of President Obama's February **Executive Order** (EO) on critical infrastructure cybersecurity. The release date was delayed nearly two weeks because of the recent government shutdown.

Notably, the PCF release now requires regulatory agencies responsible for regulating the security of critical infrastructure to assess whether they have authority to establish "requirements" based on the Cybersecurity Framework.

NIST will submit the PCF for stakeholder feedback via an upcoming 45-day comment period, as well as at an additional **workshop** November 14-15 at North Carolina State University. Venable has attended all of NIST's workshops on the Framework and will be in attendance at the upcoming workshop in Raleigh.

Few Surprises

The PCF prompted few surprises upon its release, as it reflected relatively minor changes since the **draft preliminary Cybersecurity Framework** was released in August. Examples of modifications since the last draft include:

- The addition of several new subcategories;
- The renaming of the Framework Implementation Tiers from 0-3 to 1-4; and
- The expansion and addition of citations to the privacy appendix in revision 4 of NIST's SP800-53 in the privacy protection methodology contained in the PCF's Appendix B.

NIST did not provide additional implementation guidance, but that task may ultimately be left to DHS and the other sector-specific agencies pursuant to section 8(b) of the EO.

Agency Review Process

Section 10(a) of the EO directs regulatory agencies with responsibility for regulating the security of critical infrastructure to:

- Review the PCF and "determine if current cybersecurity regulatory requirements are sufficient given current and projected risks;" and
- Within 90 days of publication, submit a report to the President that states:
  - Whether or not the agency has clear authority to establish "requirements" (based upon the Cybersecurity Framework) to sufficiently address current and projected cyber risks to critical infrastructure;
  - The authorities identified; and
  - Any additional authority required.

Although this process does not require the development of any new regulations, the same agencies are directed by section 10(b) of the EO to propose, within 90 days of publication of the final Framework, "prioritized, risk-based, efficient, and coordinated actions...to mitigate cyber risk" if the agencies determine that current regulatory requirements are insufficient. Pursuant to this directive, regulatory agencies could conceivably engage in rulemakings or other regulatory action based on the Cybersecurity Framework.

The ambiguous language used in section 10 may have been included in the EO to provide flexibility to the White House to direct regulatory mandates, but only if participation in DHS's voluntary program to adopt the Framework is regarded as insufficient, as indicated by recent statements by White House officials.

Fifth NIST Workshop

The fifth NIST workshop will cover some of the remaining logistical and other outstanding issues surrounding the Framework, including adoption considerations; considerations for small and medium

businesses; how to use the Framework; the DHS voluntary program; research and development; and "Framework ecosystem" development.

Venable will be in attendance at the workshop and will be available before and after to answer questions and address client concerns.

Liability Concerns

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 – currently set for February 12, 2014 – approaches, 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 on cyber liability management, including issues relating to insurance, the SAFETY Act, and corporate governance.

Venable will continue to closely follow NIST's progress on the development of the Cybersecurity Framework, including the upcoming workshop and public comment period on the PCF. Venable's attorneys are well-positioned to answer any and all questions on 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.