VENABLE® LLP

Cybersecurity Alert

March 2013

NIST Issues Request for Information, Begins Developing Cybersecurity Framework Under Recent Executive Order

AUTHORS

Michael J. Baader
Jamie Barnett, Rear Admiral (Ret.)
Raymond V. Shepherd, III
Anthony J. Rosso
Robert L. Smith, II
Brian M. Zimmet
Dismas Locaria
Andrew E. Bigart
Jason R. Wool
Sejal C. Shah
Amanda C. Blunt

RELATED PRACTICES

Privacy and Data Security
Communications
Homeland Security
Domain Names and Cyber Protection
Legislative and Government Affairs

ARCHIVES

2013 2009 2005
2012 2008 2004
2011 2007 2003
2010 2006

On February 26, 2013, the National Institute of Standards and Technology (NIST) issued a Request for Information (RFI) entitled, “Developing a Framework to Improve Critical Infrastructure Cybersecurity.” The RFI requests “information to help identify, refine, and guide the many interrelated considerations, challenges, and efforts needed to develop" a Cybersecurity Framework as mandated by **Cybersecurity Executive Order** 13636 issued by the Obama Administration on February 12, 2013.

The White House and NIST have repeatedly emphasized that the Cybersecurity Framework, which will serve as the cornerstone of a voluntary cybersecurity program for critical infrastructure owners and operators, will be developed through an “open public review and comment process” that will give stakeholders numerous opportunities to provide input on the standards, methodologies, procedures and processes that will make up the Framework. The RFI represents the first opportunity for public comment. Responses to the RFI must be submitted by 5:00 p.m. on April 8, 2013.

The RFI states that the Framework development process will seek to identify existing “cross-sector” cybersecurity standards and guidelines that are currently or could be applied to critical infrastructure as well as any “potential gaps (i.e., where standards/guidelines are nonexistent or where existing standards/guidelines are inadequate) that need to be addressed through collaboration with industry and industry-led standards bodies.” Further, any gaps identified will be addressed through collaboratively-developed action plans.

Although NIST admits that a one-size-fits-all Framework is not possible in light of the diversity of industries and businesses that own and operate critical infrastructure, the RFI states that “there are core cybersecurity practices that can be identified and that will be applicable to a diversity of sectors and a spectrum of quickly evolving threats.” Ultimately, the Framework is intended to include, among other mechanisms, consultative processes to assess cybersecurity-related risks and to identify security controls that would adequately address those risks, as well as “metrics, methods, and procedures that can be used to assess and monitor, on an ongoing or continuous basis, the effectiveness of security controls that are selected and deployed that can be used to facilitate continuous improvement in such controls.”

In light of these goals, the RFI seeks input from organizations on the following topics, each of which contains several questions:

. current risk management practices;
. use of frameworks, standards, guidelines, and best practices; and
. specific industry practices.

Regarding the third category, NIST requests comment on a list of potential “core” practices, including separation of business from operational systems; use of encryption and key management; identification and authorization of users accessing systems; asset identification and management; monitoring and incident detection tools and capabilities; mission/system resiliency practices; security engineering practices; and privacy and civil liberties protection.

For more information, see **Cybersecurity regulation: 5 issues for companies**.

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 these questions, and are actively monitoring related public meetings, including the Senate Commerce and Homeland Security Committees' joint hearing on the implementation of the Cybersecurity Executive Order scheduled for March 7, 2013.

For more information on how to get involved in these efforts, Venable LLP is hosting a live event/webinar, "**Cybersecurity Executive Order – A Briefing**," on **Monday, March 11, 2013 from 12:00 p.m. to 2:00 p.m. EDT**. Speakers will include numerous Venable partners with extensive experience in cybersecurity regulation and related fields. To RSVP, please **click here**.

If you have any questions concerning this alert, please contact any of the authors listed in the left rail.

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.