VENABLE® LLP

Cybersecurity Alert

February 2013

NIST Seeking Comments on Revised Standards for FISMA Compliance

AUTHORS

Michael J. Baader
Jamie Barnett, Rear Admiral (Ret.)
Raymond V. Shepherd, III
Anthony J. Rosso
Robert L. Smith, II
Dismas Locaria
Keir X. Bancroft
Andrew E. Bigart
Jason R. Wool
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 6, 2013, the National Institute of Standards and Technology (NIST) requested public comment on its latest revised draft of "**Security and Privacy Controls for Federal Information Systems and Organizations**," (Special Publication (SP) 800-53, Revision 4). Any government contractor responsible for maintaining a "FISMA compliant" information system will want to be aware of this latest revision to SP 800-53.

The Revised Draft, issued in the shadow of the President's recent Executive Order on cybersecurity, proposes various updates to the "toolbox" of risk-based cybersecurity safeguards and countermeasures that federal agencies use to protect their information systems. See **Executive Order Opens Consultative Processes to Draft Cybersecurity Framework for Critical Infrastructure** for a detailed overview of the Executive Order.

For government contractors, the Revised Draft provides a look at the future standards that federal agencies will likely impose on government contractors who have access to government information systems.

Background

Pursuant to the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347, NIST is responsible for prescribing minimum requirements for the protection of Federal information systems. Following passage of FISMA, NIST developed Federal Information Processing Standards (FIPS) 199 and 200, which, together, require subject organizations to categorize and determine the minimum security requirements for their information systems. Subject organizations must then apply SP800-53 (Revision 3 is the currently-applicable version) to create an appropriately tailored set of baseline security controls for each information system. Those prescriptions are adopted by the Office of Management and Budget (OMB), implemented by federal agencies, and flowed-down to government contractors.

Overview of NIST Recommendations for the Revised Draft

The Revised Draft sets forth an array of recommended changes, including:

- New security controls and control enhancements addressing the advanced persistent threat, supply chain, insider threat, application security, distributed systems, mobile and cloud computing, and developmental and operational assurance;
- Clarification of security control language;
- New tailoring guidance including the fundamental assumptions used to develop the security control baselines;
  Significant expansion of supplemental guidance for security controls and enhancements;
- Streamlined tailoring guidance to facilitate customization of baseline security controls;
- New privacy controls and implementation guidance based on the internationally recognized Fair Information Practice Principles;
- Updated security control baselines;
- New summary tables for security controls and naming convention for control enhancements to facilitate ease-of-use;
- New mapping tables for ISO/IEC 15408 (Common Criteria);
- The concept of overlays, allowing organizations and communities of interest to develop specialized security plans that reflect specific missions/business functions, environments of operation, and information technologies; and
- Designation of assurance-related controls for low-impact, moderate-impact, and high-impact information systems and additional controls for responding to high assurance requirements.

Placing the NIST Recommendations in Context

The Revised Draft comes at a critical and volatile juncture in the cybersecurity policy debate. Every day seems to bring new reports of cyber-attacks against U.S. government agencies or privately-owned critical infrastructure, and the resultant calls for increased cybersecurity regulation have become more frequent and insistent.

In response, on February 12, 2013, the President issued a cybersecurity Executive Order establishing a voluntary program for owners of critical infrastructure to participate in, among other initiatives, the development of a framework of cybersecurity standards. Not to be outflanked, members of Congress are working to re-introduce comprehensive cybersecurity reform legislation that stalled last year.

While the President and Congress continue to jockey for position on the issue, the Revised Draft presents concrete recommendations and more robust baseline security standards that are likely to be adopted by OMB as the successor to Revision 3. Interestingly, although the President's Executive Order requires NIST to develop a national cybersecurity framework, NIST has indicated during meetings with the public that the cybersecurity framework is more likely to resemble NIST's cloud-computing and smart grid frameworks than the standards set forth in the Revised Draft. See **Cloud Computing Synopsis and Recommendations** and **NIST Framework and Roadmap for Smart Grid Interoperability Standards**.

Thus, government contractors should monitor both the Revised Draft and NIST's efforts to develop a new cybersecurity framework to ensure that their practices and concerns are considered. For persons interested in the Revised Draft, NIST will accept comments until March 1, 2013.

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 and government contracting.