Published by *Government Contracts Law360* on February 14, 2014. Also ran in *Aerospace & Defense Law360*, *Banking Law360*, *Consumer Protection Law360*, *Energy Law360*, *Privacy Law360*, *Public Policy Law360* and *Technology Law360*.

Cybersecurity Framework May Impact Many Industries

--By Charles A. Blanchard, Kenneth L. Chernof, Ronald D. Lee, Arthur Luk, Nancy L. Perkins and Nicholas L. Townsend, Arnold & Porter LLP

Law360, New York (February 14, 2014, 4:59 PM ET) -- On Feb. 12, 2014, the White House released the final version of the cybersecurity framework developed by the National Institute of Standards and Technology.[1] The framework, which was required under the executive order President Obama issued last February after Congress failed to pass cybersecurity legislation,[2] consists of information security standards, guidelines and best practices to promote the protection of critical infrastructure.[3]

President Obama called the framework a "turning point" in "securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet," which he said "America's economic prosperity, national security, and our individual liberties depend on."[4] In large part, the final framework tracks the preliminary Framework NIST released for comment last fall,[5] with one notable exception: The draft framework contained a separate appendix devoted to data privacy and security that has been removed in the final framework.

Although the framework itself is voluntary, the standards articulated in the framework could become mandatory for some owners and operators of critical infrastructure. In exercising their authority over regulated industries, federal regulatory agencies may look to the framework in prescribing security requirements for entities subject to their jurisdiction.

In fact, President Obama's 2013 executive order requires federal agencies with responsibility for regulating the security of critical infrastructure to determine if current cybersecurity regulatory requirements are sufficient and to propose actions to address insufficiencies where necessary based on the NIST framework.[6] Already, the U.S. Department of Homeland Security has established the Critical Infrastructure Cyber Community (C3) Program as a public-private partnership to increase use of the framework, and other agencies may soon follow with analogous programs.

The framework may also impact a number of industries that are not owners or operators of critical infrastructure. For example, last August, the White House released a list of potential incentives the government may offer to encourage companies to adopt the protocols prescribed in the framework, including liability protections, cybersecurity insurance, and cybersecurity conditions in government grants.[7]

The framework consists of three components — the framework core, profiles and tiers.

- The framework core is a set of cybersecurity activities and references that are common across critical infrastructure sectors. The cybersecurity activities are divided into functions that provide company decision-makers a high-level strategic view of an organization's management of cyber risks. The five functions are expressed in terms of "to dos" — identify, protect, detect, respond and recover.

- The profiles are a guide for aligning cybersecurity activities with business requirements, risk tolerances and resources. Organizations can use the profiles to understand their current cybersecurity state, support prioritization and measure progress toward a target state.

- The tiers provide a mechanism for organizations to assess their processes for managing cyber risk. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor in risk management practices, the extent to which cybersecurity risk management is informed by business needs, and its integration into the company's overall risk management practices.

The framework also includes guidance regarding privacy and civil liberties protections related to cybersecurity activities. It notes, for example, that companies should consider incorporating "privacy principles" such as data minimization in the collection, disclosure and retention of personal information material related to a cybersecurity incident. However, as mentioned above, one key difference between the final framework and the preliminary framework that NIST released in October 2013 is that the separate appendix dealing with privacy issues, which had been a focus of criticism, was removed in favor of integrating privacy issues throughout the final framework.

Many stakeholders had focused almost exclusively on that appendix as prescribing a set of standards that would potentially be broadly applied across a wide range of entities, and the removal of the appendix would appear to reflect a need for further debate and consideration of such broadly applicable terms.

The framework is part of a larger federal government initiative to increase private sector cybersecurity. In 2013, the U.S. Department of Defense played a lead role in the Obama administration's efforts to leverage the government's buying power and existing regulatory authority to impose significant new obligations on defense contractors.[8]

Looking ahead, the NIST framework is another step toward expanding the administration's cybersecurity efforts beyond the defense industrial base to critical infrastructure providers and, eventually, large portions of the U.S. economic base.[9] According to NIST, "the Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation." To that end, NIST outlined next steps and identified key areas of development, alignment and collaboration in the "roadmap" that it released as a companion document to the framework.[10]

[1] White House Press Release: Launch of the Cybersecurity Framework (Feb. 12, 2014), available at http://www.whitehouse.gov/the-press-office/2014/02/12/launch-cybersecurity-framework.
[2] President Issues Executive Order to Improve Cybersecurity of Critical Infrastructure, Arnold & Porter LLP Advisory (Feb. 25, 2013), available at http://www.arnoldporter.com/publications.cfm?action=advisory&u=PresidentIssuesExecutiveOrdertoImproveCybersecurityofCriticalInfrastructureMembersofCongressReintroduceBiPartisanCybersecurityLegislation&id=979.
[3] Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.
[4] Statement by President Obama on the Cybersecurity Framework (Feb. 12, 2014), available at http://www.whitehouse.gov/the-press-office/2014/02/12/statement-president-cybersecurity-framework.
[5] Improving Critical Infrastructure Cybersecurity Executive Order 13636: Preliminary Cybersecurity Framework (Oct. 22, 2013), available at http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf. For additional details regarding the preliminary framework, please see our prior advisory which is available at http://www.consumeradvertisinglawblog.com/2013/10/how-is-your-business-doing-when-it-comes-to-data-security-new-national-institute-of-standards-and-te.html.

[6] Improving Critical Infrastructure Cybersecurity (Feb. 12, 2013), available at http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
[7] For additional details regarding the White House's list of potential incentives, please see our prior advisory which is available at http://www.arnoldporter.com/publications.cfm?action=advisory&u=NewGovernmentCybersecurityStandardsCouldImpactManyCompanies&id=1062.
[8] DoD issued a number of regulations in 2013 including (1) a requirement to "adequately safeguard" IT systems that contain unclassified controlled technical information, (2) a requirement to report certain cyber incidents, and (3) a new rule on mitigating supply chain risks. For additional details regarding these DoD regulations, please see our prior Advisory available at http://www.arnoldporter.com/publications.cfm?action=advisory&u=NewDoDRequirementsForDefenseContractorCyberIncidentReportingSafeguardingTechnicalInformationAndSupplyChainRisk&id=1090.
[9] For additional detail regarding other federal cybersecurity initiatives anticipated in the coming year, please see our prior Advisory available at http://www.arnoldporter.com/publications.cfm?action=advisory&u=DoDandGSAIssueRecommendationsonImprovingCybersecurityThroughAcquisition&id=1113.
[10] NIST Roadmap for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

Charles Blanchard, Kenneth Chernof, Ronald Lee and Arthur Luk are partners, Nancy Perkins is counsel, and Nicholas Townsend is an associate in Arnold & Porter's Washington, D.C., office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.