COVINGTON
COVINGTON & BURLING LLP

E-ALERT | Defense, Homeland & National Security
Government Contracts

February 13, 2014

NIST RELEASES CYBERSECURITY FRAMEWORK (VERSION 1.0) AND ROADMAP; DHS LAUNCHES CRITICAL INFRASTRUCTURE CYBER COMMUNITY VOLUNTARY PROGRAM

On February 12, the National Institute of Standards and Technology ("NIST") released its "Framework for Improving Critical Infrastructure Cybersecurity" Version 1.0 (the "Framework"). The Framework release came exactly one year after the President's Executive Order 13,636 on Improving Critical Infrastructure Cybersecurity ("Executive Order"), and follows NIST's issuance, on October 22, 2013, of a "Preliminary Cybersecurity Framework" ("Preliminary Framework").

Along with the Framework, NIST issued on February 12 a separate "Roadmap for Improving Critical Infrastructure Cybersecurity" ("Roadmap"). The Roadmap describes NIST's next steps with the Framework and provides further information about key areas for future cybersecurity development, alignment, and collaboration involving NIST and other standard-setting organizations and the private sector. In addition, to assist industry in implementing the Framework, the Department of Homeland Security ("DHS") has launched a Critical Infrastructure Cyber Community or C^3 (pronounced "C Cubed") Voluntary Program. Each of these developments is discussed further below.

BACKGROUND: PURPOSE FOR AND DYNAMIC NATURE OF THE FRAMEWORK

Pursuant to the Executive Order, which tasked NIST with developing a "Cybersecurity Framework" to "reduce cyber risks to critical infrastructure,"[1] NIST last year published a Request for Information in the *Federal Register* and received more than 200 comments from companies, unions, state and local governments, federal agencies, trade associations, and other organizations. Taking these comments and other input gained from multiple workshops, NIST released a series of drafts of the Framework from May through October 2013. Consistent throughout the development of the Framework has been the requirement in the Executive Order that the Framework must "provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk."

The Framework issued this week is identified as "Version 1.0," and is intended to be a "living document." NIST intends to hold at least one workshop within six months to "provide a forum for stakeholders to share experiences in using the Framework," as well as workshops to continue to refine the Framework. Although NIST anticipates serving in a coordinating role at least through Version 2.0 of the Framework, NIST will solicit input on options for "long-term governance of the

[1] The Executive Order defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The DHS Critical Infrastructure program identifies 16 critical infrastructure sectors here.

Framework including transitioning responsibility of the Framework to a non-government organization."

Implementation of the Framework by owners and operators of critical infrastructure is voluntary.[2] Consistent with its voluntary nature, the Framework is designed to align with the "business requirements, risk tolerances, and resources of the organization." Industry's attention, however, is likely to continue to focus on the requirement in the Executive Order for the Secretaries of DHS, Treasury, and Commerce to make recommendations regarding incentives that could be used to encourage adoption by the private sector. In August 2013, the White House released the recommendations from the three Departments. These recommendations covered eight areas: cybersecurity insurance, grants, process preference, liability limitations, streamlined regulations, public recognition, rate recovery for price-regulated industries, and cybersecurity research. The Administration has not yet released its final policy on incentivizing adoption of the Framework. Given that several of these incentives would require legislation to be realized, final implementation may not occur anytime soon.

COMPONENTS OF THE FRAMEWORK

The Framework largely tracks the Preliminary Framework that NIST released in October 2013. As in the Preliminary Framework, the Framework consists of three parts: the Framework Core, Framework Implementation Tiers, and Framework Profiles.

- The Framework Core is presented as a table at Appendix A. The Core is comprised of four elements: (1) Functions, (2) Categories, (3) Subcategories, and (4) Informative References. Functions organize basic cybersecurity activities at their highest level: Identify, Protect, Detect, Respond, and Recover. These Functions are not intended to be implemented in a serial manner, but instead are intended to be performed concurrently and continuously to address the evolving cyber threat. Each Function is broken down into Categories (*e.g.*, Asset Management, Access Control, and Detection Processes), and each Category is further broken down into specific Subcategories of technical and/or management activities. For each Subcategory, the table provides "Informative References" to particular standards or industry practices that can inform how businesses accomplish each Subcategory. Such standards include, for example, NIST Special Publication 800-53, which addresses recommended security controls for federal government systems, and ISO/IEC 27001, which addresses information security management systems.
- Framework Implementation Tiers describe the extent to which cybersecurity risk management is informed by and integrated into an organization's overall risk management practices. The Tiers are: (1) Partial, (2) Risk-Informed, (3) Repeatable, and (4) Adaptive, with the Adaptive Tier denoting the best developed risk management procedures. The Framework views these Tiers as a progression from "informal, reactive responses" to approaches that are "agile and risk-informed." The Framework notes that "[p]rogression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective" and "[s]uccessful implementation of the Framework is based upon achievement of the outcomes described in the organization's Target Profile(s) and not upon Tier determination."
- A Framework Profile combines an organization's identification of Categories and Subcategories relevant to the particular business with an assessment of which Implementation Tier the organization is currently achieving or wishes to achieve in the future with respect to each Category and Subcategory. The Profile is intended to enable an organization to establish a

[2] According to news reports and reported quotes from Administration officials, DHS does not plan to formally track which companies implement the Framework.

roadmap for addressing cybersecurity risk that is aligned with organizational and sector goals and which considers legal and regulatory requirements, industry best practices, and risk management priorities. The Framework suggests that organizations can create both a Current Profile and a Target Profile, and depending on the complexity of an organization, an organization may have multiple Profiles. The Framework does not provide a template Profile, although this could be a suggestion for future versions of the Framework.

IMPLEMENTATION OF THE FRAMEWORK AND ROLE OF DHS

Section 3 of the Framework explains different ways that an organization could use the Framework. These include (i) reviewing/comparing an organization's cybersecurity activities with those discussed in the Framework Core; (ii) using the Framework to create a Current Profile and Target Profile, and an action plan to reach the Target Profile; (iii) using the common language provided by the Framework to communicate cybersecurity requirements to external service providers (*e.g.*, a cloud provider to which the organization is exporting data) or other parties; and/or (iv) identifying opportunities for standards bodies or other organizations to develop new or revised Informative References.

As we have described previously, the Framework is likely to be most relevant to owners and operators of critical infrastructure. To this end, DHS has launched a Critical Infrastructure Cyber Community ("C³") Voluntary Program, with a principal focus on engaging with Sector-Specific Agencies (SSAs) and other organizations using the Framework to develop guidance for the implementation of the Framework. DHS has said that it hopes ultimately to expand the program to "all critical infrastructure and businesses of all sizes that are interested in using the Framework."

For businesses that are not subject to sector-specific regulators, the Cybersecurity Framework is unlikely to have a direct impact. However, over time, the Framework could lead to a set of cybersecurity standards that courts or regulators might regard as defining a reasonable standard of care. In addition, businesses may wish to implement the Framework and participate in the C³ Voluntary Program for various other reasons, including (i) taking advantage of participation incentives, (ii) because participation becomes a *de facto* requirement to be awarded certain government contracts, and/or (iii) because implementation proves to be an effective approach to improving a company's cybersecurity (which in turn helps to protect proprietary information from cyber threats and/or protects against the reputational, financial, legal and other damage that can be caused by data breaches).

PRIVACY AND CIVIL LIBERTIES

The Preliminary Framework included an appendix entitled, "Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program." Such a methodology is required by Section 5 of the Executive Order, which requires agencies to incorporate privacy and civil liberties protections into their activities. This appendix provided specific methodologies and Informative References for particular Functions and Categories from the Framework Core.[3]

The appendix, with its detailed table, has been removed from the Framework. Instead, the Framework includes a more general discussion within the body of the Framework. The Framework notes that "[p]rivacy and civil liberty implications may arise when personal information is used, collected, processed, maintained or disclosed in connection with an organization's cybersecurity activities." To address privacy issues, the Framework suggests that an organization consider how its cybersecurity program may incorporate privacy principles related to data minimization, use

[3] The Preliminary Framework explained that "[e]very Category may not be represented as not all Categories give rise to privacy and civil liberties risks."

limitations, transparency, individual consent and avenues for redress and others. In addition, the Framework notes various processes and activities — such as cybersecurity personnel with privacy responsibilities reporting to appropriate, trained management; taking steps to identify and address privacy implications of access control measures; and informing cybersecurity service providers about an organization's privacy policies— that an organization could consider to address privacy and civil liberty issues.

In the Roadmap that accompanies the Framework, NIST states that it will host a privacy workshop, focused on identifying technical standards and best practices to mitigate the impact of cybersecurity activities on individuals' privacy and civil liberties, in the second quarter of 2014.

AREAS FOR FUTURE ACTION

In addition to describing procedural next steps, the Roadmap describes several substantive "high-priority areas for development, alignment, and collaboration" with particular sectors and standards-developing organizations. Among other areas, these relate to the development of better identity and authentication mechanisms, automated sharing of cybersecurity threat indicators, conformity assessment mechanisms, data analytics, and supply chain risk management. NIST describes these areas a non-exhaustive list identified by stakeholders that should inform future versions of the Framework.

We are well-positioned to assist clients in understanding the implications of the Cybersecurity Framework on their businesses, including whether and how to implement the Framework and/or to participate in the C^3 Voluntary Program.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Defense, Homeland & National Security, Government Contracts and Public Policy & Government Affairs practices:

David Fagan	+1.202.662.5291	dfagan@cov.com
Susan Cassidy	+1.202.662.5348	scassidy@cov.com
James Garland	+1.202.662.5337	jgarland@cov.com
Roger Zakheim	+1.202.662.5959	rzakheim@cov.com
Gabriel Slater	+1.202.662.5159	gslater@cov.com
Kristen Eichensehr	+1.202.662.5312	keichensehr@cov.com
Anuj Vohra	+1.202.662.5362	avohra@cov.com
Catlin Meade	+1.202.662.5889	cmeade@cov.com

This information is not intended as legal advice. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP, an international law firm, provides corporate, litigation and regulatory expertise to enable clients to achieve their goals. This communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts.