COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Defense, Homeland & National Security

September 4, 2013

NIST RELEASES DISCUSSION DRAFT OF PRELIMINARY CYBERSECURITY FRAMEWORK

On August 29, the National Institute of Standards and Technology ("NIST") issued a "Discussion Draft of a Preliminary Cybersecurity Framework" pursuant to the President's Executive Order 13,636 on Improving Critical Infrastructure Cybersecurity. The NIST is drafting the Framework in consultation with industry, other government agencies, and other experts, and the "Discussion Draft" was released in advance of a cybersecurity workshop that will be held next week in Texas. The formal "draft" of the Framework is due out in October, and the final Framework is required to be adopted by February 2014 — one year from the issuance of the Executive Order.

While the "Discussion Draft" provides, as its name suggests, an important preliminary preview of the Framework envisaged by the NIST, the Framework may evolve before it is finalized. Nevertheless, because the release by the NIST offers the first public preview of the potential Framework, it may be of particular interest to clients and other parties that are monitoring U.S. cybersecurity policy and regulation. The remainder of this alert summarizes the Discussion Draft.

THE PURPOSE FOR AND DEVELOPMENT OF THE FRAMEWORK

The Executive Order tasked NIST with developing a "Cybersecurity Framework" "to reduce cyber risks to critical infrastructure." The Order specifies 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 is intended to provide the roadmap for the voluntary adoption of cybersecurity practices by owners and operators of critical infrastructure. Specifically, after the final Framework is issued, the Secretary of Homeland Security, along with sector-specific agencies, must establish a "voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure." The Secretary of Homeland Security is also directed to "coordinate establishment of a set of incentives" to promote participation in the voluntary program by critical infrastructure owners and operators.

THE FRAMEWORK'S PROVISIONS

As described by the NIST discussion draft, the Framework is intended to guide businesses through a risk-based assessment and improvement of their cybersecurity posture. The discussion draft Framework is organized around three issues: the Framework Core, Implementation Tiers, and Profile.

- The Framework Core includes five functions: identify, protect, detect, respond, and recover. Each function is tied to categories of activities that address cybersecurity risk, including, for example, access control and data security. Each category includes references to particular standards or

industry practices that can inform how businesses accomplish each function. Such standards include, for example, NIST Special Publication 800-53, which addresses recommended security controls for federal government systems.

- Framework Implementation Tiers describe the sophistication of risk management an organization chooses to apply to each category of action. The tiers include partial, risk-informed, repeatable, and adaptive levels, with the "adaptive" tier denoting the best developed risk management procedures.
- The Framework Profile combines the selection of the categories of activities in the Framework Core that are relevant to a 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. The draft Framework suggests that organizations create both a current profile and a target profile to assist organizations in improving cybersecurity by moving toward their target profile.

APPLICATIONS OF THE FRAMEWORK

In addition to the draft of the Framework itself, NIST released a discussion draft of illustrative examples of how businesses could use the Cybersecurity Framework in response to particular scenarios. In particular, the examples walk through application of the Framework to mitigating cybersecurity intrusions, combating malware, and addressing insider threats.

Relatedly, Appendix B to the discussion draft provides a "methodology to address privacy and civil liberties considerations" that arise as businesses implement the Framework. The discussion draft addresses how organizations can safeguard personally identifiable information while performing the five functions of identify, protect, detect, respond, and recover.

As we have described previously, the Framework is likely to be most relevant to owners and operators of critical infrastructure. Section 9 of the Executive Order directs the Secretary of Homeland Security to "use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic, or national security." Although the compliance with the Framework is generally voluntary, critical infrastructure entities may be directly regulated by their sector-specific agencies. Section 10 of the Executive Order directs sector-specific agencies that regulate critical infrastructure to report to the President on "whether the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure" and "any additional authority required."

Entities that are not critical infrastructure, but nonetheless have sector-specific regulatory agencies, may also be impacted. The Order authorizes sector-specific agencies to "develop implementation guidance or supplemental materials to address sector-specific risks and operating environments." Agencies may extend any such guidance or supplemental materials based on the Framework beyond critical infrastructure to all entities that they regulate.

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 *de minimis* set of reasonable practices. Alternatively, businesses may wish to adopt the Framework and participate in the voluntary program contemplated by the Order, particularly if the incentives for such participation are attractive.

AREAS FOR POSSIBLE FUTURE ACTION

In accordance with the Executive Order, the discussion draft Framework also identifies "areas for improvement" that NIST may address in future collaborations with standards-developing organizations or specific sectors. High priority areas for improvement include identity authentication, automated sharing of cybersecurity threat indicators, standardized methods for protecting individual privacy, and managing supply chain risk.

As noted, NIST is expected to issue a formal preliminary Cybersecurity Framework in October.

We are well-positioned to assist clients in understanding the impact of the Executive Order, including the ongoing Cybersecurity Framework development process, on their operations and in considering whether to participate in the voluntary program that the Order envisions.

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

Michael Chertoff	+1.202.662.5060	mchertoff@cov.com
Jon Kyl	+1.202.662.5660	jkyl@cov.com
David Fagan	+1.202.662.5291	dfagan@cov.com
Richard Hertling	+1.202.662.5669	rhertling@cov.com
Kristen Eichensehr	+1.202.662.5312	keichensehr@cov.com