COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Defense, Homeland & National Security

November 4, 2013

NIST RELEASES PRELIMINARY CYBERSECURITY FRAMEWORK

On October 22, the National Institute of Standards and Technology ("NIST") released a "Preliminary Cybersecurity Framework" pursuant to the President's Executive Order 13,636 on Improving Critical Infrastructure Cybersecurity. NIST has published a request for comments on the Preliminary Cybersecurity Framework in the Federal Register and set a due date of December 13 for all comments. NIST also will host another in its series of workshops to discuss the Framework on November 14 and 15 at North Carolina State University.

NIST has been drafting the Framework in consultation with industry, other government agencies, and other experts, but the 45-day comment period represents an important final opportunity for the private sector to weigh in on the Framework before NIST publishes the final version in February 2014 in accordance with the deadline set by Executive Order 13,636.

THE PURPOSE FOR AND GENESIS 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."

In releasing the Preliminary Framework, NIST explained that it "offers a common language and mechanism for organizations to determine and describe their current cybersecurity posture, as well as their target state for cybersecurity" and "will help [organizations] identify and prioritize opportunities for improvement within the context of risk management," as well as helping them to "assess progress toward their goals." The Preliminary Framework itself states that one of its "key objective[s]" is to "encourage organizations to consider cybersecurity risk as a priority similar to financial, safety, and operational risk while factoring in larger systemic risks inherent to critical infrastructure."

Adoption of the Final Framework by owners and operators of critical infrastructure will be voluntary, though government-sponsored incentives will encourage its adoption. The Executive Order directs the Secretary of Homeland Security, along with sector-specific agencies, to establish a "voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure." It also directs the Secretary of Homeland Security to "coordinate establishment of a set of incentives" to promote participation in the voluntary program by critical infrastructure owners and operators. In August, the White House released a preliminary list of possible incentives, including considering adoption of the Framework in criteria for government grants, providing limitations on liability, and providing public recognition of companies that adopt the Framework. The "voluntary program" will be finalized after publication of the Final Framework.

THE FRAMEWORK PROVISIONS

The Preliminary Framework largely tracks the discussion draft that NIST released at the end of August. As we noted in our prior alert on the discussion draft, the 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 "Informative 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, and ISO/IEC 27001, which addresses information security management systems.
- Framework Implementation Tiers describe the sophistication of risk management an organization chooses to apply to each category of action. The tiers include: (1) partial, (2) risk-informed, (3) risk-informed and repeatable, and (4) adaptive, 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 Preliminary 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.

The Framework explains that it "provides a common language to communicate requirements among independent partners responsible for the delivery of essential critical infrastructure services," including, for example, cloud services providers.

IMPLICATIONS AND APPLICATIONS OF THE FRAMEWORK

In addition to the substantive portions of the Framework, Appendix B to the Preliminary Framework provides a "methodology to address privacy and civil liberties considerations" that arise as businesses implement the Framework. The Framework provides a methodology and Informative References that organizations can use to 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 less likely to have a direct impact. However, the Framework may provide such entities with a way of organizing and evaluating the cybersecurity threats that they confront — and developing their own safeguards to address and respond to such threats. The Framework also provides another data point for 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 Preliminary 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. The Preliminary Framework adds another area — development of a skilled cybersecurity workforce — that was not addressed in the discussion draft and specifically explains that "greater attention is needed" to develop resources "to raise the level of technical competence of those who build, operate, and defend systems delivering critical infrastructure services."

As noted, NIST plans to issue the final Cybersecurity Framework in February 2014.

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, Public Policy & Government Affairs, and Government Contracts 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
Roger Zakheim	+1.202.662.5959	rzakheim@cov.com
Robert Nichols	+1.202.662.5328	rnichols@cov.com
Susan Cassidy	+1.202.662.5348	scassidy@cov.com
Richard Hertling	+1.202.662.5669	rhertling@cov.com
Kristen Eichensehr	+1.202.662.5312	keichensehr@cov.com