"'Framework' Heralds New Era for Cyber Security," GPM Privacy Alert

March 20, 2014

PRIVACY ALERT - NIST: FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE

On February 12, 2014, the Department of Commerce's National Institute of Standards and Technology released its Framework for Improving Critical Infrastructure (Version 1.0). The Framework is the result of President Obama's 2013 Executive Order on "Improving Critical Infrastructure Cybersecurity" that called for a voluntary risk-based set of industry standards and best practices to help organizations manage cybersecurity risks. The Framework heralds a new era in cybersecurity - federally endorsed cybersecurity procedures and practices for private industry and organizations. In a nutshell, here's what you need to know.

How it works: The Framework is designed to complement (not replace) existing cybersecurity programs. It is a risk-based approach to reducing cybersecurity exposure, which consists of three main elements:

- **Core -** "A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes." It identifies specific industry standards and guidance to achieve those outcomes. The Core comprises four types of elements: Functions (basic cybersecurity activities), Categories, Subcategories and Informative References. There are five Functions designed to assist an organization in understanding its cybersecurity program (Identify, Protect, Detect, Respond and Recover). Categories are subdivisions of a Function grouped into cybersecurity outcomes. Subcategories divide a Category into specific outcomes of technical and/or management activities. An Informative Reference is a specific section of standards, guidelines, and common practices that illustrate a method to achieve the outcomes associated with each Subcategory.
- **Implementation Tiers -** These "provide context on how an organization views cybersecurity risk and the processes in place to manage that risk." The Tiers range from "Partial" (Tier 1) to "Adaptive" (Tier 4) and describe an "increasing degree of rigor and sophistication in cybersecurity risk management practices."
- **Profile -** A Profile "enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities." Basically, the Profiles can be used to identify opportunities for improving cybersecurity be comparing a Current Profile with a Target Profile. Successful implementation of the Framework is based on achievement of the outcomes described in the Target Profile, not the Tier determination. Importantly, the Framework provides a common language to communicate requirements among interdependent parties. In that regard, the Framework notes that an "organization may utilize a Target Profile to express cybersecurity risk management requirements to an

external service provider (e.g., a cloud provider to which it is exporting data)."

- Consensus Development: The Framework is the result of a year-long effort to gather input from a broad range of industries and provides a "consensus description of what's needed for a comprehensive cyber security program." Accordingly, the Framework reflects real-life experiences of those grappling with today's cybersecurity threats. It relies on standards, guidelines and best practices currently available to evaluate and mitigate cybersecurity risks.

Flexible and Scalable: Although ostensibly aimed at financial, energy, health care and other critical infrastructure sectors, NIST explains that the Framework "allows organizations - regardless of size, degree of cyber risk or cybersecurity sophistication - to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure." The Framework recognizes that organizations have unique risks and that they can they can determine which activities are important and prioritize expenditures to maximize the effect of each dollar spent.

Voluntary: Adoption and implementation of the Framework is voluntary. Nevertheless, the consensus standards and best practices may ultimately serve as a benchmark for establishing the standard of care for purposes of legal liability. In the event of a cybersecurity event, liability may turn on whether and the degree to which a company implements the Framework. Moreover, and as noted above, a Target Profile may soon become a way of communicating uniform cybersecurity requirements to providers of essential critical infrastructure services.

Global Reach: The Framework references globally accepted standards, guidelines and practices. As a result, "organizations domiciled inside and outside of the United States can use the Framework to efficiently operate globally and manage new and evolving risks." NIST notes that the Framework "will discourage balkanization caused from unique requirements that hamper interoperability and innovation, and limit the efficient and effective use of resources." Consequently, implementation of the Framework may ultimately improve efficiency and reduce costs for cross-border transactions and relationships.

Privacy and Civil Liberties: As required by the Executive Order, the Framework provides a short description of a methodology to protect privacy and civil liberties. In that regard, the Framework only provides a "general set of considerations and processes" as these concerns may differ by sector or over time and organizations may use varying processes to address these concerns. Generally, the Framework indicates that in appropriate circumstances, a cybersecurity program might incorporate certain privacy principles. Among other things, an organization may consider whether various processes are in place to ensure compliance with privacy laws, regulations, Constitutional requirements and the organization's privacy policies.

Incentives for Implementation: President Obama's Executive Order also called for establishment of a set of incentives designed to promote participation in the cybersecurity program. The process of identifying the

incentives is still underway, but the White House has already previewed some possibilities. At the top of the list is Cybersecurity insurance. A White House spokesperson explains that the goal of collaborating with the insurance industry "would be to build underwriting practices that promote the adoption of cyber-risk reducing measures and risk-based pricing and foster a competitive cyber insurance market." This highlights the importance of insurance in managing cyber-related risks. Moreover, availability and premiums for coverage may very well depend on an organization's Implementation Tier and Profile.

Future Developments: The Framework is intended to be a "living document" and as such will continue to evolve over time. In that regard, NIST released a "Roadmap" that "lays out a path toward future framework versions and ways to identify and address key areas for cybersecurity development, alignment and collaboration." Some of the high-priority areas for future activities include: better identity and authentication solutions; automated sharing of indicator information; leveraging existing conformity assessment programs; secure application of "big data" analytic techniques; determine the key challenges to supply chain risk management to enable more effective Framework implementation; and improvements in the protection of individuals' privacy and civil liberties while securing infrastructure.

If you have any questions about the content of this privacy alert, please contact Nick Nierengarten at 612.632.3040 or nicholas.nierengarten@lathropgpm.com.