Client Alert

pillsbury

Energy

Privacy, Data Security & Information Use

Cybersecurity

Global Sourcing

February 18, 2014

National Cybersecurity Framework Released – Has Your Organization Considered the Implications?

By Catherine D. Meyer, Meighan E. O’Reardon, Deborah S. Thoren-Peden, and Amy L. Pierce

*On February 12, 2014, the National Institute of Standards and Technology (“**NIST**”) released the final version of its Framework for Improving Critical Infrastructure Cybersecurity (the “**Cybersecurity Framework**” or “**Framework**”) and the companion NIST Roadmap for Improving Critical Infrastructure Cybersecurity (the “**Roadmap**”). The final version is the result of a year-long development process which included the release of multiple iterations for public comment and working sessions with the private sector and security stakeholders. The most significant change from previous working versions is the removal of a separate privacy appendix criticized as being overly prescriptive and costly to implement in favor of a more general set of recommended privacy practices that should be “considered” by companies.*

The Cybersecurity Framework marks an important step for U.S. cybersecurity policy after an Executive Order from the Obama Administration called for its creation in February 2013.[1] While use of the Cybersecurity Framework is voluntary, the Federal government has been actively exploring various measures to incentivize participation both universally and on a sector-by-sector basis.[2] While the Framework is focused on the 16 sectors identified as critical infrastructure,[3] companies outside those areas can use the Framework in their risk assessment and enterprise security planning.

[1] *See* Executive Order 13636 “Improving Critical Infrastructure Cybersecurity”, February 12, 2013.

[2] *See* http://m.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework. See also Incentives Study Analytic Report, Department of Homeland Security, June 12, 2013 available at https://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf.

[3] The 16 critical infrastructure sectors are chemical, commercial facilities, communications, critical manufacturing, dams, defense, emergency services, energy, financial services, food and agriculture, government facilities, health, information technology, nuclear, transportation, and water.

What is the Cybersecurity Framework?

The Cybersecurity Framework is a risk management tool to assist companies with assessing the risk of cyber-attack, protecting against attack, and detecting intrusions as they occur. According to NIST, it complements, but does not replace, an organization's existing risk management processes and cybersecurity program. It is organized into three parts – the Framework Core, the Framework Implementation Tiers, and the Framework Profile. The Framework was developed by leveraging existing cybersecurity standards, guidelines and practices. Organizations are encouraged to use it as a tool to continuously assess and improve (where appropriate) cybersecurity practices.

The Framework Core is comprised of five key functions: Identify, Protect, Prevent, Respond, and Recover. These functions are intended to organize companies' basic cybersecurity activities at the highest level and represent a lifecycle for managing cybersecurity across an organization. Each function is further broken down into categories and subcategories that highlight the more detailed processes and activities associated with managing cybersecurity. As set forth in the Cybersecurity Framework, examples of the categories under each function include:

> **Identify**: Asset Management, Business Environment; Governance; and Risk Assessment
>
> **Protect**: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology
>
> **Detect**: Anomalies and Events; Security Continuous Monitoring; and Detection Processes
>
> **Response**: Response Planning; Communications; Analysis; Mitigation; and Improvements
>
> **Recover**: Recovery Planning; Improvements; and Communications

The Cybersecurity Framework includes a maturity model that is characterized by implementation "Tiers" for companies to use to assess their progress and development across the various functions. The tiers involve characterizing an organization's development as Partial, Risk-Informed, Repeatable, or Adaptive behavior. Partial maturity is characterized by informal and occasional implementation of the Framework, meaning that the organization is unlikely to have processes in place to utilize cybersecurity information. Risk-Informed entities will have formal, risk-aware processes defined and implemented. An organization that has achieved the Repeatable stage of maturity will have validated processes that are responsive to larger enterprise requirements and needs. Finally, entities that are considered Adaptive will be able to anticipate challenges, adapt rapidly and manage risk in conjunction with changes.

Under the Cybersecurity Framework, assessing an organization's functions in relation to the maturity or implementation Tiers and risk tolerance results in its Profile. NIST encourages companies to use the profile to identify gaps and develop action plans to improve cybersecurity.

Criticisms

The Cybersecurity Framework has been criticized as being overly broad and toothless. Some security professionals note that the Framework is not that different from the checklists that chief security officers already regularly implement. Most large organizations have already implemented a risk management process similar to the Cybersecurity Framework to manage their cybersecurity activities. And, in practice medium and smaller sized organizations may benefit most significantly from this first version of the Cybersecurity Framework. However, additional sector-specific iterations are anticipated and many government analysts note that the Cybersecurity Framework has the potential to become the de facto standard for managing cybersecurity risk.

What's next for U.S. Cybersecurity Policy?

The companion Roadmap to the Cybersecurity Framework outlines several planned follow on activities. In the near term, NIST will continue to oversee and coordinate the ongoing development of the Cybersecurity Framework including by accepting informal comments on the recent release. Additionally, a workshop will be held in the next six months for stakeholders to share feedback on their use of the Cybersecurity Framework. Options for long term governance including identifying the appropriate responsible partners(s) for overseeing the Cybersecurity Framework are also being solicited. Finally, the Roadmap identifies nine cybersecurity disciplines marked for further development and discussion including: (i) authentication; (ii) automated indicator sharing; (iii) conforming cybersecurity assessments; (iv) preparation of a skilled cybersecurity workforce; (v) use of data analytics in cybersecurity; (vi) Federal agency cybersecurity alignment; (vii) international coordination; (viii) supply chain risk management; and (ix) technical privacy standards.

How Can Your Organization Use the Cybersecurity Framework?

Regardless of whether your company falls within one of the defined critical infrastructure sectors, the Framework can be a valuable tool for cross-checking and testing your existing cybersecurity risk management programs. The Framework provides granularity that can be useful in each phase of your program.

Financial services businesses covered by the Gramm-Leach -Bliley Act have guidance in the form of the Standards for Safeguarding Customer Information (Safeguarding Rule) and the Interagency Guidance on Response Programs that require implementation of an information security program including conducting an annual risk assessment, assess the sufficiency of any safeguards in place to control the identified risks, training employees, reviewing information systems (network and software as well as processing, storage, transmission and disposal), detecting, preventing and responding to intrusions or system failures, and overseeing vendors and service providers.

Similarly, companies that are covered entities under the Health Insurance Portability and Accountability Act (HIPAA) have fairly specific regulations governing security of protected health information.

Companies outside financial services and healthcare that comply with the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth (201 Mass. Code Regs. § 17.00) will have implemented a written data security plan that meets the requirements of that regulation, including designating a responsible employee, conducting a risk assessment, implementing an employee security policy, enforcing the policies, addressing issues surrounding terminated employees, overseeing and requiring compliance by service providers, limiting the amount of information collected, limiting retention of data, data mapping, restricting access to records, monitoring performance, reviewing the program annually and implementing an incident response plan.

For each of these businesses, the Cybersecurity Framework addresses additional areas where threats may exist and additional specific steps that can be taken to better protect the business. While the Framework is not designed to replace an information security program, certain aspects of the Framework may trigger improvements in a company's program that help meet the business' strategic priorities: protecting assets and business viability against loss, achieving the appropriate level of security commensurate with the security and scope of the company's data, protecting company systems and data against threats to the network structure and security, anticipating evolving threats to the company's systems and meeting the company's regulatory compliance obligations.

If you have any questions about the content of this alert, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Catherine D. Meyer (bio)
Los Angeles
+1.213.488.7362
catherine.meyer@pillsburylaw.com

Deborah S. Thoren-Peden (bio)
Los Angeles
+1.213.488.7320
deborah.thorenpeden@pillsburylaw.com

Meighan E. O'Reardon (bio)
Washington, DC
+1.202.663.8377
meighan.oreardon@pillsburylaw.com

Amy L. Pierce(bio)
Sacramento
+1.916.329.4765
amy.pierce@pillsburylaw.com

This publication is issued periodically to keep Pillsbury Winthrop Shaw Pittman LLP clients and other interested parties informed of current legal developments that may affect or otherwise be of interest to them. The comments contained herein do not constitute legal opinion and should not be regarded as a substitute for legal advice.