crowell moring

CLIENT ALERT

NIST Releases Cybersecurity Framework

Feb.12.2014

After a year of development, NIST has released the long-awaited Cybersecurity Framework, which promises to have significant implications for the public and private sectors alike. The final version retains much of the Framework Core set forth in the draft version and provides a blueprint to align cybersecurity efforts (along with the accompanying Roadmap document with next steps), but many questions remain, including further defining voluntary adoption and incentives for adoption, the impact on government contracting, and how the standard may be used by third parties – and those questions will likely continue to drive further development of the Framework.

The Framework is one of the defining initiatives of President Obama's Executive Order 13636 for Improving Critical Infrastructure Cybersecurity, issued in February 2013, which recognized cyber threats as "one of the most serious national security challenges we must confront." The Order thus instructed the National Institute of Standards and Technology (NIST) to develop a set of voluntary standards and processes that private industry, particularly critical infrastructure, could use to address these cyber risks. NIST issued a preliminary draft in October 2013, and after receiving public comments and holding several workshops, issued the final version on February 12, 2014.

In its final form, the Framework features considerable industry input, reflecting the Order's goal of establishing "voluntary consensus standards and industry best practices to the fullest extent possible." Consequently, the Framework provides "a prioritized, flexible, repeatable, performance-based, and cost-effective approach" that the private sector can use to identify, assess, and manage its cybersecurity risks. It also emphasizes the need for senior executive involvement, elevating cyber risk management from what was once thought to be an IT department issue to a broader enterprise issue.

The Framework Core

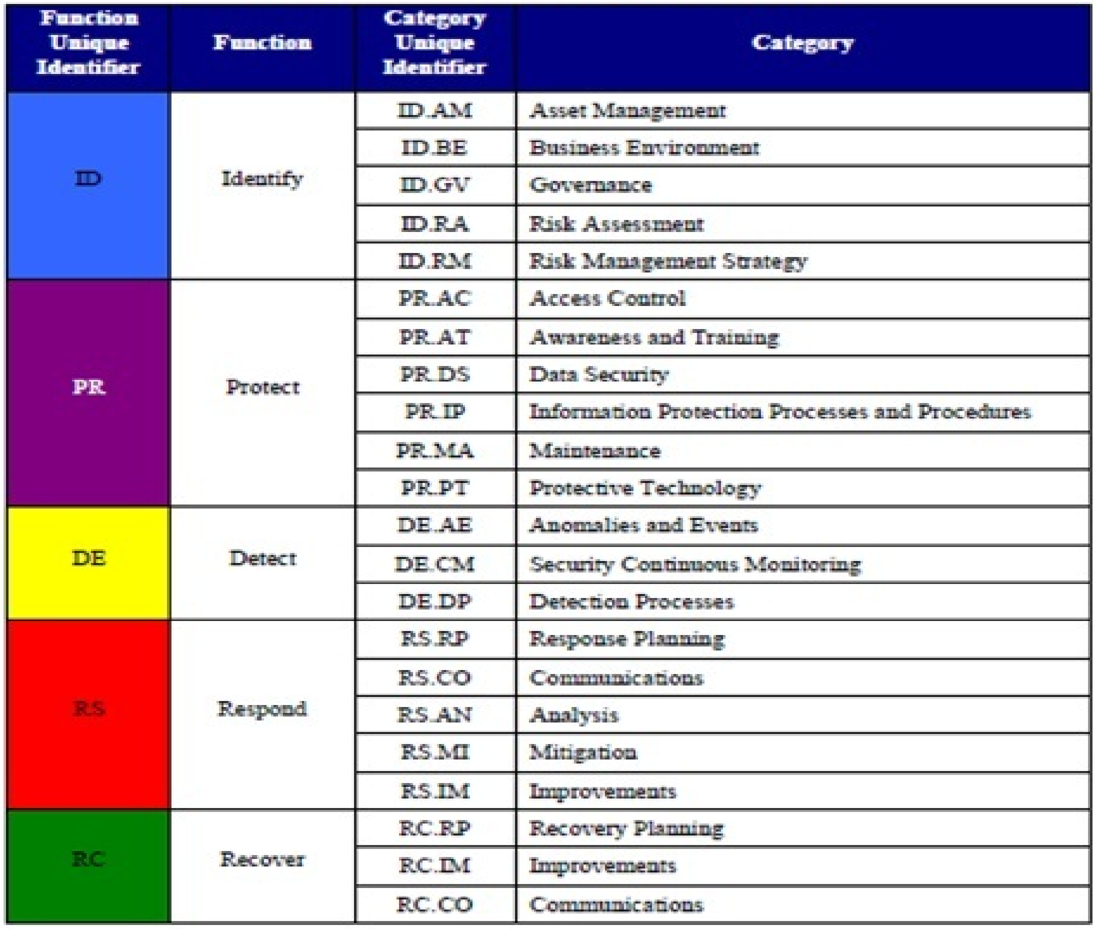
The main structure of the standard is the "Framework Core." Here, NIST outlines the five primary functions necessary for cyber resilience, as well as what kinds of actions each function may entail:

- **Identify**: Managing assets, such as personnel, systems, and facilities; understanding the company's business environment; implementing policies and procedures to ensure both security and legal compliance; conducting a risk assessment; and managing risk appropriately.
- **Protect**: Controlling access to information and facilities; informing and training employees and business partners; securing data in accordance with the company's risk strategy; implementing policies and procedures to secure data, including physical security, data destruction, and incident response plans; and adopting technical solutions to support data security efforts.
- **Detect**: Adopting processes to timely detect anomalous activity and to then appropriately respond; continuous monitoring to detect cybersecurity events and to identify vulnerabilities; and testing those processes and monitoring techniques.

- **Respond**: Implementing a response plan during or after an event; ensuring that event response activities are coordinated between internal and external stakeholders; analyzing an incident's cause and impact; containing and eradicating incidents; and updating response plans based on lessons learned.
- **Recovery**: Utilizing a plan to restore systems; improving recovery plans by incorporating lessons learned; and managing public relations in a coordinated fashion after an event.

In conjunction with these functions, the Core also provides "Informative References" that cite to external standards, such as ISO and NIST Special Publications, that contain further details.

Table 1: Function and Category Unique Identifiers



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Source: NIST Framework For Improving Critical Infrastructure Cybersecurity, v. 1.0 (Feb. 12, 2014) at p. 19.

Privacy Considerations

Notably absent from the final version of the Framework is the Privacy Appendix B set forth in the draft version. The Appendix was originally intended "to protect individual privacy and civil liberties" by mapping Framework Core provisions to standards such as the Fair Information Practice Principles (FIPPs). As NIST stated in a January 15, 2014 update, however, public comments indicated that this "methodology did not reflect consensus private sector practices and therefore might limit use of the Framework." As a result, NIST eliminated the Appendix in favor of more general guidance that focuses on ensuring proper privacy training, reviewing any monitoring activities, and evaluating any privacy concerns that arise when sharing information (such as threat data) outside the company.

Impact on Government Contracting

As another key directive, EO 13636 required DoD and GSA to make recommendations "on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration." The resulting November 2013 report provides six recommendations, with the most notable being the development of baseline cybersecurity requirements as a condition for contract award and the establishment of common cybersecurity definitions for federal acquisitions. This is an area where there will be continued actions and activities to follow. Given the current patchwork of cybersecurity standards among the federal agencies, some centralized guidance may contribute greater consistency, lesser compliance burdens, and improved security for both agencies and contractors.

"Implementation Tiers" Remain (With Modification)

Despite initial criticism, the Framework retains the "Implementation Tiers" classification system that provide context on how an organization views cybersecurity risks and the associated processes in place to manage those risks. The Tier structure progresses from "Partial" (Rank 1) for informal and reactive cybersecurity programs, to "Adaptive" (Rank 4) for agile and risk-informed programs. Although NIST encourages Tier 1 organizations to consider moving to higher Tiers, the Framework emphasizes that Tiers do not represent "maturity levels" and that "[s]uccessful implementation of the Framework is based on outcomes described in the organization's Target Profile(s) and not upon Tier determination." In turn, the "target profiles" – which NIST does not define – represent the outcomes needed to achieve the desired cybersecurity risk management goals. In other words, the Framework proposes that companies utilize "Implementation Tiers" to assess current cybersecurity efforts and "Target Profiles" to identify goals as a mechanism to reveal gaps to be addressed.

Looking Ahead

The release of the Framework and Roadmap both serves as the end of the process commenced by the President's signing of EO 13636 and the beginning of implementation and further refinement of the Framework. Key areas that will continue to be closely analyzed and followed include:

- What constitutes voluntary adoption?
- What are the incentives for adoption?
- Will the Framework serve as a standard of care?
- What is the impact on regulations?

- Will there be corresponding legislation?

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

David Z. Bodenheimer
Partner – Washington, D.C.
Phone: +1 202.624.2713
Email: dbodenheimer@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

Kate M. Growley, CIPP/G, CIPP/US
Partner – Washington, D.C.
Phone: +1 202.624.2698
Email: kgrowley@crowell.com