Government Affairs & Public Policy

ASIS INTERNATIONAL
Advancing Security Worldwide®

NIST Releases Cybersecurity Framework

Briefing Paper for the ASIS International CSO Roundtable

After a year in development, the National Institute of Standards and Technology (NIST) has released the long-awaited Cybersecurity Framework, which promises to have significant implications for the public and private sectors alike. The final version of the Framework provides a blueprint for critical infrastructure businesses to align cybersecurity efforts and bolster resilience.

Background

The Framework was initiated by President Obama's Executive Order 13636 for Improving Critical Infrastructure Cybersecurity, issued in February 2013. The Order instructed NIST to develop a set of voluntary standards and processes that private industry, particularly critical infrastructure, could use to address 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 and the 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 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 suspicious activity and then to 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 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; updating recovery plans by incorporating lessons learned; and managing public relations in a coordinated fashion after an event.

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

Privacy Considerations

An earlier draft version of the Framework contained the Privacy Appendix B, which is absent from the final version. The intent was to "protect individual privacy and civil liberties" by linking the Framework Core to standards such as the Fair Information Practice Principles (FIPPs). NIST issued an update in January 2014 stating that 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 proper privacy training, reviewing monitoring activities, and evaluating any privacy concerns when sharing information (such as threat and vulnerability data) outside the company.

Implementation Tiers

Despite initial criticism, the final Framework includes an "Implementation Tiers" classification system that provides context on how an organization views cybersecurity risks and the associated processes in place to manage those risks. The Tier structure ranges from "Partial" (Tier 1) for informal and reactive cybersecurity programs, to

"Adaptive" (Tier 4) for agile and risk-informed programs. Although NIST encourages Tier 1 organizations to consider moving to higher Tiers, the Framework emphasizes that "successful implementation of the Framework is based on outcomes described in the organization's Target Profile(s) and not upon Tier determination." Though not defined by NIST, Target Profiles represent the outcomes needed to achieve a desired level of cybersecurity risk management. In short, the Framework suggests that companies utilize the Tiers to assess current cybersecurity efforts and Target Profiles to identify goals and security gaps to be addressed.

Next Steps for the Framework

The final Framework is intended to be a living document and includes a Roadmap identifying next steps. While the release of these final documents serves as the end of the process commenced by the Executive Order, it is just the beginning of implementation and further refinement of the Framework. As discussed in the Roadmap, key areas that will continue to be closely 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?