White House Cybersecurity Framework Takes a Cajoling Tone

Posted At : February 21, 2014 9:36 AM | Posted By : John Slye
Related Categories: Critical Infrastructure Protection, Department of Homeland Security, Homeland Security, Innovation, Information Security, Cybersecurity, Policy & Legislation

Last week the White House unveiled its much-anticipated framework for cybersecurity aimed at persuading financial, energy, and other critical infrastructure companies to further bolster their network protections against cyber- attacks. The measured tone of the guidance and accompanying statements by officials is a stark contrast to the Obama Administration's aggressive posture at the onset of the initiative.

The Framework for Improving Critical Infrastructure Cybersecurity is the product of a year-long effort led by the National Institute of Standards and Technology (NIST) initiated by President Barack Obama's Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013. While the release came within the Obama's specified time frame initial news reaction was that the framework was much weaker than what he promised a year ago. The White House's promotion voluntary standards is a marked departure from the more regulatory approach it had pursued up to this point and in his published statement on its release the President said that much more work needs to be done.

Framework Overview

The Framework describes itself as a risk-based approach to managing cybersecurity risk and seeks to reinforce the connection between business drivers and cybersecurity activities. Its core is composed of three parts:

- **The Framework Core** – a set of five cybersecurity functions—Identify, Protect, Detect, Respond, Recover, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level.
- **Framework Implementation Tiers** – describes the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive) measured over a range, from Partial (Tier 1) to Adaptive (Tier 4), from informal to agile and risk-informed.
- **A Framework Profile** – the alignment of current standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state).

The remainder of the Framework defines cyber- risk management and further discusses the three Framework components, with examples of how the Framework can be used, and provides additional reference information relevant to implementation.

White House Event and DHS Program

The White House announced the Framework release with an event that featured speakers from several agencies and a panel of industry advocates that have worked closely with the administration on the issue. A key repeated theme throughout was the voluntary nature of the Framework, which may be a reaction to concerns that federal policy in this area would pursue a heavy-handed regulatory bent.

As part of the roll-out, The **Department of Homeland Security** Secretary Jeh Johnson announced the launch of their Critical Infrastructure Cyber Community C³ Voluntary Program, a public-private partnership aimed at aligning critical infrastructure owners and operators with existing resources that will help them adopt the Framework and manage their cyber risks. The stated primary goals of the C³ Voluntary Program are to support industry in increasing cyber resilience, to increase awareness and use adoption of the Cybersecurity Framework, and encourage organizations to manage cybersecurity as part of an all hazards approach to enterprise risk management. In his remarks, Johnson said one aspect of the C-cubed program includes providing industry access to cyber- experts at DHS for consultation and advice at no cost.

Also at the event, Department of Commerce Secretary Penny Pritzker chaired a **panel of supportive industry execs** from AT&T, Lockheed Martin, and PEPCO to show their support for the White House's efforts. Among their comments, they emphasized the "good first step" aspect of the framework and that it is not a "cookie-cutter" approach. They also stressed the fact that "there are no truly private networks" as well as the need to understand exactly what actors and devices are connected to their networks.

White House **Cyber Coordinator Michael Daniel** closed out the event by highlighting the intent to continue to foster C-level engagement in order to keep the Framework a living document through NIST workshops, etc.; to address the regulatory aspects of the EO by streamlining and aligning existing regulations without issuing new ones; and to deal with the issue of incentives for industry to participate in the framework and related cyber- efforts.

Implications

In the industry panel discussion, AT&T's Randall Stephenson commented that he sees huge opportunities within the cyber framework for big business. He and the others see the **need for innovation** in cybersecurity, including solutions that improve an organization's situational awareness of their cyber- risk posture, training and education, policy development and enforcement, risk management, etc. It was unclear whether he meant up-side for cybersecurity vendors or potential for big firms to improve their cyber- risk poster, or both.

The **potential cost** of pursuing the government's framework approach has been raised as an issue. In fact, an administration official noted that the federal government is going to "do its best to make the costs of using the framework lower, and the benefits of the framework higher…"

Cybersecurity opportunities that develop within the private critical infrastructure markets will complement the ongoing needs of federal agencies to secure their networks and improve their processes, especially in light of the continued **challenges and failures** of many agencies to lead by example.

---
*Originally published for Federal Industry Analysis: Analysts Perspectives Blog. Discover more about **GovWin FIA**. Follow me on Twitter **@GovWinSlye**.*