Cyber Framework Shifts toward Standards Implementation

Posted At : November 4, 2013 4:51 PM | Posted By : Kyra Fussell
Related Categories: Critical Infrastructure Protection, Information Security, Cybersecurity, Department of Commerce

Earlier this fall, White House Cybersecurity Coordinator Michael Daniel wrote that, "Cyber is one of those challenging areas in which there really is no 'done.'" This is a particularly poignant observation as we look at government-industry collaboration and progress in developing security standards. A few days after Daniel posted that blog, the National Institute of Standards and Technology (NIST) released the next draft of the cybersecurity framework for critical infrastructure providers.

NIST released the *Preliminary Cybersecurity Framework* on Tuesday, October 22, 2013. Comments will be accepted over the next few months before Version 1.0 of the framework is completed in February 2014. The next workshop for the framework has been scheduled for mid November. Early in this process, a question about best practices was raised. Namely, what has prevented industry from sharing and changing their practices? While no definitive answer was achieved, the role of security within various business organizations has no doubt in play. As organizations look to balance business goals with security objectives, risks weigh differently for different organizations. Ultimately, the cybersecurity framework will have a different impact for organizations of differing size and market sector. The preliminary draft notes that, "The Frame work complements, and does not replace, an organization's existing business or cybersecurity risk management process and cybersecuity program."

As for encouraging adoption, over the summer, the administration referenced potential incentives associated with the framework, including insurance, grants, streamlined regulations, and public recognition. While several of these can be implemented now, others will follow completion of the framework. It's worth noting that reception of these incentives is likely to vary across industries. For example, some industries are already regulated by government agencies, such as banking. As review of the framework continues, the extent of the agencies' regulatory authority will need to be determined. Within the insurance industry, government agencies and providers are collaborating to ensure the framework can be properly utilized. These initial discussions precede any formal recommendations or policies, which are likely to hinge on the finalized framework.

The fifth workshop for the framework will be held November 14 to 15 in Raleigh, North Carolina. According tothe draft agenda, this workshop will explore implementation as well as future information security governance. Amid ongoing federal spending pressure, government contractors look for business opportunities in the private sector resulting from new security standards. Further exploration of how these standards may be implemented will shed some light on where some of those opportunities may arise.

Originally published for Federal Industry Analysis: Analysts Perspectives Blog. Stay ahead of the competition by discovering more about GovWinIQ. Follow me on Twitter @FIAGovWin.