INSIDE CYBERSECURITY
News and analysis on evolving federal policies to protect cyberspace

Industry consortium nears completion of 'Cybersecurity Discovery Process'

Posted: October 11, 2013

Inside Cybersecurity -- A major industry consortium is nearing the completion of a comprehensive "discovery process" companies and government agencies can use to wade through hundreds of cybersecurity standards and guidelines and decide which matter most to them.

The Network Centric Operations Industry Consortium's Cybersecurity Discovery Process will allow users to answer a myriad of questions, including "why companies are or are not investing in cybersecurity protections, what incentives would encourage them to do so, and what's the viability of a particular business model relative to cybersecurity markets," said Mark Bowler, chair of NCOIC's technology council.

"How do you encourage those companies, those entities, those organizations to find the right way for them to be protecting their networks, and what's going to motivate them to do so?" he asked in an interview with Inside Cybersecurity. "How can we encourage them to make the right investments?"

NCOIC bills itself as a "collaboration of premier leaders in the aerospace, defense, information technology, large-scale integrator and services industries" that focuses on interoperability among industries, companies and other entities.

A key component of the NCOIC process is a massive database of cybersecurity "policies, laws, regulations, standards, best practices and guidelines" not unlike the compendium being compiled by the National Institute of Standards and Technology as part of the framework of voluntary standards it is developing.

Bowler said the NCOIC database contains more than 700 entries, more than twice what NIST's includes. But, he said, the goal is not to compete with NIST; rather, NCOIC has offered to share its database with the government.

"We have the same standards in there, but our focus is a little bit different, so we're not trying to replicate their database or take it over," he said. "We have offered to NIST to cooperate on the database; we're still exploring that option. . . . We're certainly happy to let NIST publish it and maintain it."

NCOIC has been working with NIST and other participants in the process of writing the voluntary framework, which is due out in preliminary form once as the government shutdown ends. A final framework is due by February 2014.

Bowler said the NCOIC discovery process should be released early in 2014 as well. It will be made available to anyone who wants to use it, though Bowler said it is not likely to be a "self-serve tool that you could simply go off and execute."

Instead, NCOIC envisions companies and other entities approaching the consortium for help answering a question or a set of questions related to cybersecurity. "We think we add value in being the originators of the process," Bowler said. "The consort would add value if an organization, government or otherwise, wanted to have the process executed for them; they could come to the consortium to have it done."

The process, he added, "is kind of broad in the sense that you can ask it any number of questions, and you need to know what you want to investigate before you get started," he said. A company might want to use the process to determine the "most relevant standards and best practices" needed in its sector, for example.

Another question the process could help an entity answer: "What's the consequences of particular policies or laws or regulations . . . on the marketplace?"

The process has been tested in various workshops run by NCOIC, Bowler said. It will be described in a white paper NCOIC plans to publish within the next few weeks.

Dan Dupont (ddupont@iwpnews.com)