ODNI Working With DoD to Strengthen Insider Threat Workforce

NEWS
EMERGING TECH
CYBERSECURITY

Aug 7, 2018 | 5:49 pm

Wayne Belk, director of the National Insider Threat Task Force (NITTF), said today at an event hosted by Nextgov and Equifax that his unit in the Office of the Director of National Intelligence is now working with the Defense Department to clarify and strengthen the roles of the Federal government's insider threat staff, beginning with its security analysts.

"One of things that we're doing, we're in partnership with the Office of the Under Secretary of Defense for Intelligence to develop a certification program for insider threats within the U.S. government," Belk said.

He explained that the new program is being developed in phases, beginning with the insider threat analysts in charge of investigating threats and making sense of vast troves of actionable but admittedly disparate data.

“The whole point is a professionalized insider threat workforce in the U.S. government,” Belk said. He added, “I can tell you for sure, I will not see that the rest of my career,” but said his organization was “in the process of snapping on the first layer of Legos” and that with “every piece you snap on, you get a little bit closer to the finished product.”

NITTF–a unit within the National Counterintelligence and Security Center–was established in October 2011 under President Obama’s executive order (EO) aimed at combating insider threats in the wake of the disclosure of U.S. secrets to WikiLeaks.

Belk explained that the EO gave instructions to “build a government-wide program to deter, detect, and mitigate the insider threat.” He called those goals “three separate phases of the problem,” where resources need to be adequately allocated. Belk said that focusing on one aspect instead of all three is a cause for concern, but indicated that deterrence–preventing a potential threat actor from reaching “that fork where they make the wrong decision”–was an important place to situate many of those resources.

For those security analysts looking to sort out disparate data sets, Belk noted that the challenge is clear. “You don’t necessarily want every single piece of information about everybody,” he said.

And when advanced detection, audit, and activity monitoring data identify that a user has “done something strange,” he said it is simply that–an isolated, strange incident, but not one that necessarily implies guilt or commission of a crime.

“You have to have a sense of what all of that means,” Belk said. The challenge then comes with being able to “pull together all of the disparate data sources that you need, and then pull together all of the relevant authorities to leverage it,” he said.

Creating a professionalized staff to execute on that mission may take longer than Belk’s remaining tenure, but the reasoning for that goal is clear. Belk quipped that the threats they’re tackling won’t be going anywhere soon.

“As long as there have been two people keeping a secret, there’s been an insider threat problem,” he said.