Homeland Security begins sharing cyberthreats with business

March 17 2016, by Tami Abdollah

In this Jan. 13, 2015 file photo, President Barack Obama speaks at the National Cybersecurity and Communications Integration Center in Arlington, Va. The Homeland Security Department opened up shop Thursday as a portal for sharing cyber threats with the private sector and the rest of government—a culmination of a longtime bipartisan effort to improve information flow and cybersecurity. (AP Photo/Evan Vucci)

The Homeland Security Department on Thursday formally began sharing

details of new digital threats with private business and other government agencies, a culmination of a longtime effort to improve cybersecurity.

"This is the 'if you see something, say something' of cybersecurity," said Homeland Security Secretary Jeh Johnson at the agency's Virginia-based data sharing hub, the National Cybersecurity and Communications Integration Center.

A federal law passed at the end of 2015 was intended to encourage corporations to share information about cyberthreats, making it harder for businesses to be targeted by threats used elsewhere.

The program is voluntary, and the number of companies that will participate or how effective the program will be remains unclear.

Companies have long been reluctant to acknowledge security failures. As of Thursday, about six organizations had signed up and others have expressed interest, Andy Ozment, the assistant cybersecurity secretary at Homeland Security, said. The names of companies participating are closely held, and records about their involvement are exempt from disclosure under the Freedom of Information Act.

"This is a big deal," he said. "We're not going to launch out the gates ... and have thousands of companies sharing all sorts of information. We want to make sure we're providing value and growing."

Under the new law, the Homeland Security Department programmed its systems to remove personally identifiable information that might be included that private companies might share.

"As companies come on board, we'll learn more about what's useful," and learn to streamline other parts, said Suzanne Spaulding, a top Homeland Security cyber official.

If information pertains to a specific threat of economic damage, death or serious injury or the effort to prosecute or prevent the exploitation of a minor, personal information may be passed on to other agencies.

Information sharing and analysis centers, which industry groups operate, will likely participate in the new program, DHS officials said. Johnson said he was telling such groups, "We are open for business, on time and on schedule."

Rep. Michael McCaul, R-Texas, chairman of the House Committee on Homeland Security, praised the new effort following recent hacks against Sony Pictures Entertainment Inc. and the Office of Personnel Management. More than 21 million Americans had their personal information stolen in the OPM hack, which the U.S. believes was a Chinese espionage operation.

 More information: Cyber threat sharing program information: www.us-cert.gov/ais

Citation: Homeland Security begins sharing cyberthreats with business (2016, March 17) retrieved 13 March 2024 from https://phys.org/news/2016-03-homeland-cyberthreats-business.html