

US Congress wants hack teams for self-penetration

While girding power grid

By Dan Goodin

1st May 2009 19:03 GMT

The United States Congress this week delved further into the country's cybersecurity preparedness as members introduced two bills designed to protect federal networks and electric power grids from attacks.

One bill, dubbed the US Information and Communications Enhancement Act of 2009, would mandate the formation of hacker teams that would actively try to penetrate government networks. Current laws focus more on generating reports that detail vulnerabilities and defenses to them than putting security into practice, many security experts say.

Sponsored by Senator Tom Carper of Delaware, the bill would also establish a National Office for Cyberspace that would be responsible for carrying out cybersecurity policy. Additionally, it would create a council of chief information security officers who would stay in touch with CISOs from each federal agency to share information about the latest threats.

A separate bill introduced this week by Representative Bennie Thompson of Mississippi is aimed at strengthening the US power grid against attack. The so-called Critical Electric Infrastructure Protection Act would give federal regulators more power to respond to emergencies involving infrastructure that transmits electricity. Among other things, the Federal Energy Regulatory Commission could issue "emergency rules or orders" when an attack is imminent.

The bills come three weeks after a separate piece of legislation was introduced in the Senate that would give the president unprecedented authority over the nation's critical infrastructure, including the power to shut down or limit traffic on private networks during emergencies.

While by no means perfect, the flurry of bills is a cause for hope, some security experts believe.

"My reaction to all of these is that it seems the nation has reached a tipping point - Congress is speaking for the country saying this problem is bad enough to act - CSIS said we are losing the cyber wars," Alan Paller, director of research for the SANS Institute, wrote in an email, referring to a recent report by the Center for Strategic and International Studies. "Urgency is high. It is time to stop talking and start fixing."