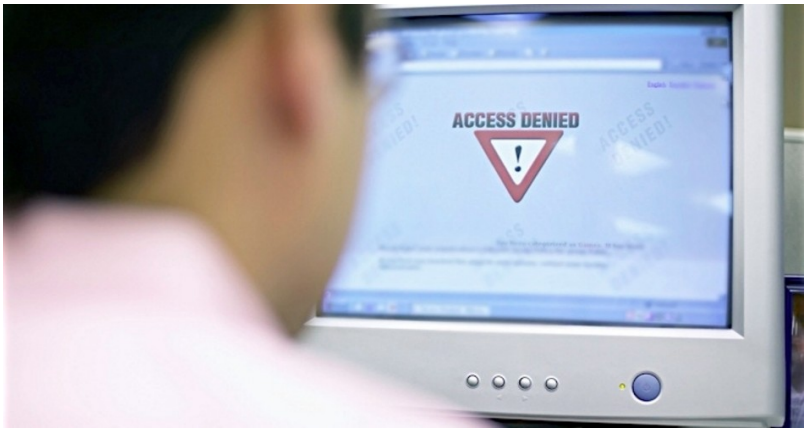
Written by **Kurt Hyde** on August 14, 2012

Internet Regulation Still a Threat in the 112th Congress



Freedom advocates breathed sigh of relief when a coalition of Senate Republicans and a few Democrats opposed the Cybersecurity Act of 2012 (S. 3414). Unfortunately, the recent setback of the Cybersecurity Act of 2012 has all the earmarks a false sense of security. The timing has created a false impression that Internet regulation legislation has failed for this session of Congress, but the 112th Congress is virtually certain to convene a lame duck session after the election.

If anyone thinks a lame duck session is only a minor concern, the lame duck session of 2010 should serve as a warning. The outgoing congressmen, predominantly Democrats, submitted a blizzard of bills. The Senate Republicans had enough votes to stop every one of the bills. The voters gave a mandate for change at the ballot boxes that November. All the Senate Republicans needed to do was to stand with the American people and block those bills in the Senate. Instead they chose to pretend they were powerless. They fiddled while America's freedom burned. There doesn't appear to be any evidence a lame duck session in 2012 would be much different than the lame duck disaster of 2010.

Regulating the Internet appears to be a top priority for the liberals and neocons in Washington. The Internet has become the main medium of communication for many politically minded people. While the use of the Internet is open to people of all political persuasions, it has become the most important means of communicating for many advocates of return to constitutional government.

Public outcry stopped, at least temporarily, the Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA). But an even worse bill, the Cyber Intelligence Sharing and Protection Act (CISPA) passed the House and is now waiting for action in the Senate.

The Cybersecurity Act of 2012 was the worst bill of them all. It would create a National Cybersecurity Council. Among the numerous unconstitutional provisions of the National Cybersecurity Council would be to:

> "coordinate the adoption of private-sector recommended voluntary outcome-based cybersecurity practices."

The U.S. Constitution does not authorize any such power, not even for voluntary practices. Of course, anyone who has witnessed governmental power grow via patient gradualism realizes that voluntary is just a stepping stone on the path to mandatory. Such a council would be constitutional if its scope were limited to protecting the federal government's computers and computer networks. It would be constitutional for the federal government to share appropriate threat information with the public in a manner similar to that of FBI Law Enforcement Bulletins as practiced during the tenure of J. Edgar Hoover. It is amazing how many of the stated goals of the Cybersecurity Act of 2012 could be accomplished without violating the US Constitution, but the contents of the bill go far beyond what the US Constitution allows.

Section 601 of the Cybersecurity Act of 2012 refers to the Council of Europe's Convention on Cybercrime, which was ratified as a treaty by the US Senate in 2006. Further provisions in the bill regarding cybercrimes, in addition to being unconstitutional, would also ensnare us in a maze of international law.

The Cybersecurity Act of 2012 lists as its justification some of the well-known threats that could befall us in the event of an E-attack, such as "interruption of life-sustaining services, including energy, water, transportation, emergency services, or food" and "failure or substantial disruption of a financial market." These threats, listed in the bill dated July 19, 2012, are remarkably similar to those listed in an article in *The New American* online published approximately four months earlier on March 9, 2012.

While the description of the threats may be similar to those in *The New American* online article, the proposed solutions in the Cybersecurity Act of 2012 are vastly different. Instead of admitting the role played by government in putting us in jeopardy in case of an E-attack, the Cybersecurity Act of 2012 just ignores that aspect. Instead of starting the corrective action by undoing as much as possible of governmental causes of the problems, the solutions listed in the bill are more government regulation, more internationalism and less freedom of the Internet.

What Government Has Done To Make Us Vulnerable?

As mentioned in *The New American* article of March 9, 2012, many of the security weaknesses in our computer infrastructure have been caused by government. Whether that be the federal government's upstaging of the private sector in computer networking by funding ARPANET, immigration policies that allow people from high-risk of terrorism foreign nations to be in this country, legally or illegally, or affirmative action laws that frequently give these people advantages over loyal Americans in hiring, governmental involvement has been part of the problem all along.

Let's look at just a few of the threats listed in the Cybersecurity Act of 2012:

Energy — That's a part of our economy that is excessively regulated. Just one aspect of energy is the delivery of electricity and natural gas to many homes and businesses is via public utility companies that are regulated by government agencies. Why haven't the well-paid government regulators of these utility companies required the utility companies to have contingency plans to deal with the possibility of an Internet interruption, temporary or extended?

Water — For most American homes and businesses, their water is supplied by government. Why aren't they prepared for an Internet interruption?

Emergency Services — In most communities these are run by government agencies from local all the way up to FEMA at the federal level. Why aren't they prepared for an Internet interruption?
Instead of using these vulnerabilities as a springboard to further increase government regulation and reduce freedom, why aren't we questioning the roles of central planners and the whole idea of government regulated monopolies? Constitutionalists have frequently argued that government regulation of monopolies doesn't really make the monopolies serve the people. This may be the perfect time to reopen that debate.

While the Cybersecurity Act of 2012 has supposedly been defeated, some of the senators who opposed it are sponsoring an amendment to the bill that would make it look more like a previously submitted bill, the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information and Technology Act of 2012 (S. 3342) also known as SECURE IT.

SECURE IT, while not as obviously offensive as the Cybersecurity Act of 2012, is still unconstitutional and would lead to regulation of the Internet. Instead of creating a National Cybersecurity Council, it defines a term, Cybersecurity Center, which includes a number of military and civilian agencies. This accomplishes similar goals while opening the door to military involvement in regulating the Internet. The bill also defines requirements for security clearances for certain access. Employers, private as well as public, have traditionally controlled access to sensitive information. But codifying this into federal requirements for government security clearances strengthens the already unconstitutional federal involvement in the process as well as adding to the military nature of how it would be administered. SECURE IT could easily serve as the framework to be amended piece-by-piece to eventually include the most odious provisions of other Internet regulation bills.

The biggest threats of passage of Internet regulation legislation are the lame duck session of Congress or the aftermath of an E-attack, similar to how the Patriot Act was enacted during the aftermath of 9-11. The American people must be awakened to both of these threats or the Internet will be unconstitutionally regulated.