Written by **C. Mitchell Shaw** on September 2, 2015

Cybersecurity Info Sharing Act: Gov't Fails Security; Wants More Power

Riding in the wake of the worst cyber-attacks the world has ever seen comes the federal government's solution. The Cybersecurity Information Sharing Act (CISA) is the "new and improved" version of the same old legislation Congress has been trying to pass for years. CISA closely resembles the Cyber Intelligence Sharing and Protection Act (CISPA), which was soundly defeated in 2012 after major opposition from nearly the entire Internet community.

CISPA has returned — in spirit at least — in the form of CISA because the powers in Washington that want to codify the surveillance culture never seem to give up. The ostensible reason for this new attempt at passing this legislation is that government agencies and major corporations alike have been the targets of incredibly sophisticated cyberattacks over the past several months. Never mind that the reason many of those attacks were successful — especially those on government networks — was insufficient security measures in the first place. Nothing in CISA would do anything to protect against attacks that are the result of poor adherence to established security protocols.

The New American has reported on hacks of government systems that could have been prevented if those in charge of protecting those systems had simply done their jobs. The federal government has also failed to identify the perpetrators of hacks on major U.S. companies, instead placing the blame on others for political reasons.

Almost a year ago, a computer network at the White House was penetrated by Russian hackers. It is almost certain that those hackers were working for Moscow. One of the most disturbing elements in this case is that the hacking was not even discovered by the White House: An "ally" made U.S. officials aware of it. Within days, it was revealed that the problem of Russian hackers attacking U.S. targets was far worse than previously thought. Hackers — again with ties to the Kremlin — had succeeded in inserting a major virus, known as BlackEnergy, into key systems in both government and industry, threatening the very infrastructure of the United States.

In both of cases, the initial penetration was accomplished by users opening attachments in "phishing e-mails" from the hackers. Better training, filters, firewalls, and other security measures could have prevented the attacks. At the very least, computer security personnel should have discovered the hackers' activities much sooner than was the case.

Then, in January 2015, a hacker group calling itself Cyber Caliphate hacked the Twitter and YouTube accounts for the U.S. military Central Command and posted pro-Islamic State messages and videos. President Obama's response? He released a statement saying that this "goes to show how much more work we need to do" where cybersecurity is concerned. CISA is apparently part of that "much more work."

About the same time all that was happening, Sony Pictures became the victim of the largest hack at that point in history, with more than 100 terabytes of data exfiltrated from its systems before those systems were destroyed by hackers. While security experts and all the credible evidence pointed to an inside job and a group of "hackivists" who even claimed credit, Obama and the FBI blamed North Korea.

Again, Obama used that cyberattack to claim that he and his administration needed more authority to address the problem. He learned well from his mentor and friend Rahm Emanuel, who famously once said, "You never want a serious crisis to go to waste…. This crisis provides the opportunity for us to do things that you could not before."

Much of the common thread connecting all these events is a culture of surveillance that weakens computer security. When security holes are allowed to exist so that governments and corporations have an easier means of spying on people, hackers have a much easier time hacking. Instead of taking the advice of experts in the field of computer security, Obama and his allies in government have chipped away at privacy and liberty to continue perpetrating that surveillance culture.

Even when it was revealed that the Office of Personnel Management (OPM) had replaced Sony as the "hacking victim of all time" — with more than 22 million Americans' personal information stolen by hackers associated with Beijing and two class action lawsuits resulting from the federal government's failure to protect that data — all Obama could really muster was to propose new "cyber-laws" that will bring Congress "out of the Dark Ages." Of course, that means more control and power for government, and less freedom for citizens who use the Internet. It means laws such as CISA.

So what we have here is government failing to do what it is supposed to do. In these cases, government's roles are simple: protect government computer systems and investigate crimes against those systems and others. Having failed miserably at those tasks, the federal government now wants to use that failure to offer a "solution" that grants itself more power at the expense of Americans' freedom. This is, as 19th-century French economist Frédéric Bastiat called it, government "concocting the antidote and the poison in the same laboratory."

The White House is throwing its full weight behind CISA, saying, "Cybersecurity is an important national security issue and the Senate should take up this bill as soon as possible and pass it."

The Electronic Frontier Foundation (EFF) calls the proposal "a surveillance bill in disguise," saying the way to stop it is by repeating the efforts that effectively quashed it in its former iteration:

> Americans keep hearing that CISA and the other "cybersecurity" bills moving through Congress are "must-pass" legislation. But just like the original version of CISA — the Cyber Intelligence Sharing and Protection Act (CISPA) — grassroots activism can also stop this proposal in its tracks.

Hopefully EFF is right and sufficient pressure can be brought to bear once again to scuttle this bill.

The federal government needs to focus on the powers enumerated in Article 1, section 8 of the Constitution. Since spying on the American people and controlling the Internet are not on that list, CISA/CISPA proposals need to be put away for good. If America can move away from the culture of surveillance, it's just possible that something can be done to secure this nation's systems.