Written by **Joe Wolverton, II, J.D.** on September 13, 2012

Leaked Executive Order Gives Feds Control Over Cybersecurity

"Stroke of the pen, law of the land … kinda cool." This nugget spoken by former Clinton adviser Paul Begala seems more than anything to be the guiding principle of the Obama administration.

As is being widely reported, the White House is currently drafting an executive order giving the Department of Homeland Security (DHS) power to establish standards of cybersecurity purportedly protecting the "U.S. power grid from electronic attacks."

BusinessWeek describes the new program as a "a council that would work with the National Institute of Standards and Technology to establish the cybersecurity standards."

Of course, the information being leaked about the proposed edict makes it clear that the adoption of such standards will be voluntary.

The threshold question that arises from the announcement of such a radical step toward federal control over our information infrastructure is not being answered. That is: Is the power grid of the United States being regularly attacked?

In a word: no. As Michael Tanji of *Wired* pointed out in a recent article refuting the government's insistence that we are the target of frequent cyberattacks, "To start, these systems are rarely connected directly to the public internet. And that makes gaining access to grid-controlling networks a challenge for all but the most dedicated, motivated and skilled — nation-states, in other words."

Contrast Tanji's take on the "problem" with this story from Nextgov.com:

> Nations are increasingly employing computer attacks without "any sense of restraint," a National Security Agency official said on Friday at a forum in New York.
>
> "We're starting to see nation-state resources and expertise employed in what we would characterize as reckless and disruptive, destructive behaviors," Debora Plunkett, head of NSA's Information Assurance Directorate, told an audience at the Polytechnic Institute of New York University, Reuters reported.
>
> Players are carrying out computer espionage-related tasks with an unprecedented amount of latitude, she indicated, saying that the threat of security breaches caused by groups affiliated with China and Russia are "significant." Even during the Cold War, blocs of nations affiliated with the United States or the Soviet Union worked to undermine each other, but operated with a sense of restraint, she said, according to the article.

U.S. government officials know a little something about state-sponsored cyber attacks on the electronic infrastructure of another country.

Recently, stories have been leaked detailing the U.S. government's creation and implementation of two

such cyberattacks.

"Flame" was the name of a computer virus reportedly developed and launched by the United States in order to glean critical data from computers in several Middle Eastern countries.

According to a story published in the *Washington Post*, the United States and Israel launched a joint venture to develop the Flame virus. Once launched into cyberspace, the code reportedly collected online intelligence data that was then used to create a similar bit of malware that would cripple Iran's nuclear capabilities. Officials cited in the *Post* article revealed that the effort was a collaboration of the National Security Agency (NSA), the CIA, and the Israeli military.

One product of that Israeli-American secret enterprise was the Stuxnet virus, which was allegedly deployed by the United States to decelerate Iran's progress toward the development of a nuclear weapon.

Apparently, Flame and Stuxnet were just the beginning of a more sophisticated and sustained American cyberassault against the Iranian nuclear infrastructure. As one source quoted by the *Washington Post* reports: "This is about preparing the battlefield for another type of covert action," said one former high-ranking U.S. intelligence official, who added that Flame and Stuxnet were elements of a broader assault that continues today. "Cyber-collection against the Iranian program is way further down the road than this."

Perhaps it is our government's experience with launching such attacks that has created the potential for cyber-blowback. Put simply: Our government's targeting of the internet grid of other countries turns our own infrastructure into a target for retaliation.

If one is to believe the propaganda put out by DHS, there is a vast army of hackers with tools sophisticated enough to bring down our power grid, our water treatment centers, and our nuclear power plants. DHS insists that the number of such attacks are rising every year.

What's the upshot of the DHS report on hacking of the "companies that control our critical infrastructure?" Read the following statement from a CNN story covering the report:

> The Department of Homeland Security sees the rise in the number of reported events as a sign that businesses are trusting the government more when it comes to allowing federal investigators to access their systems.

Trusting the government to protect these systems by giving them control over them. That is the real reason for the as yet unsuccessful bills proposed in Congress that would increase the government's command and control of the electronic grid — including the Internet — and that is the aim of the as yet unsigned cybersecurity executive order.

In fact, it is likely the failure of the legislative branch to gain that control that prompted President Obama to begin prepping an executive order accomplishing the same or similar ends.

"The administration is contemplating using an executive order because it isn't clear Congress would pass a cybersecurity bill," reports *BusinessWeek*.

"An executive order is one of a number of measures we're considering as we look to implement the president's direction to do absolutely everything we can to better protect our nation against today's cyberthreats," said White House spokeswoman Caitlin Hayden. "We are not going to comment on ongoing internal deliberations."

With the very real threat of the issuance of an executive order to fight off the unsubstantiated threat to

our national cyber safety, President Obama is once again usurping legislative powers that are not his. Article I of the Constitution makes it very clear that all national legislative power resides in Congress.

Perhaps President Obama is not familiar with this warning from influential French philosopher Baron de Montesquieu:

> When the legislative and executive powers are united in the same person, or in the same body of magistrates, there can be no liberty; because apprehensions may arise, lest the same monarch or senate should enact tyrannical laws, to execute them in a tyrannical manner.

Lastly, as with most of similar plans by the federal government to scare citizens of this country straight into the protective arms of Big Brother, someone is profiting from the fear.

As *Reason* magazine reported last year:

> The U.S. government is expected to spend $10.5 billion a year on information security by 2015, and analysts have estimated the worldwide market to be as much as $140 billion a year. The Defense Department has said it is seeking more than $3.2 billion in cybersecurity funding for 2012.

On September 11 the Associated Press reported it obtained a draft of the cybersecurity executive order. According to the AP story the draft follows the lines leaked last week regarding the creation of an "infrastructure cybersecurity council manned by the US Department of Homeland Security that will be staffed by members of the departments of defense, justice and commerce, and national intelligence office."

Photo: Thinkstock