Written by **Joe Wolverton, II, J.D.** on November 10, 2012

Is Obama's Cybersecurity Executive Order Imminent?

Flush with electoral capital, President Barack Obama is spending it like mad in pursuit of his radical power consolidating agenda. Over the past few days we have chronicled the fast-tracking of a UN gun control treaty, the prosecution of another alleged espionage case, another deadly drone attack, approval of a planned UN invasion of Mali, etc.

The latest stop of the Barack Obama Worldwide Tour of Tyranny may be the issuing of a long-awaited and regularly leaked executive order exerting control over the Internet in the name of cybersecurity.

Of course, there remains the chance that Congress will pass some version of a cybersecurity bill before the president can issue his edict. Congress will be back in town on November 13 and Republican leaders have already telegraphed their intent to "reach across the aisle" and accede to the president's mandate, including the touting of ObamaCare as "the law of the land."

Then again, the president famously declared that "we can't wait" for Congress to act, and given the fact that there are a few other pretty weighty items on the legislative schedule, a cybersecurity executive order isn't out of the question. The decree would take that topic off Congress's plate and allow the president greater control over the scope and severity of the regulations governing the "protection" of the nation's cyberspace infrastructure.

Promises of the White House's imminent issuing of the edict have been coming for months. The Associated Press (AP) obtained a leaked draft version of the order, but indicated that the source of the document didn't disclose when the president would sign the order.

Greater evidence of the imminent issuing of the order came on September 19, when Department of Homeland Security Secretary Janet Napolitano said the executive order granting the president sweeping power over the Internet is "close to completion."

In testimony before the Senate Committee on Homeland Security and Governmental Affairs, Napolitano said that the order is still "being drafted" and vetted by various high-level bureaucrats. But she also indicated that it would be issued as soon as a "few issues" were resolved. Assuming control of the nation's Internet infrastructure is a DHS responsibility, Napolitano added.

"DHS is the Federal government's lead agency for securing civilian government computer systems and works with our industry and Federal, state, local, tribal, and territorial government partners to secure critical infrastructure and information systems," she informed senators.

Napolitano's report on the role of DHS squares with the information revealed in the seven-page version of the order the AP has read. According to the report of their findings:

> The draft order would put the Department of Homeland Security in charge of organizing an information-sharing network that rapidly distributes sanitized summaries of top-secret intelligence

> reports about known cyberthreats that identify a specific target. With these warnings, known as tear lines, the owners and operators of essential U.S. businesses would be better able to block potential attackers from gaining access to their computer systems.

The new draft, which is not dated, retains a section that requires Homeland Security to identify the vital systems that, if hit by cyberattack, could "reasonably result in a debilitating impact" on national and economic security. Other sections establish a program to encourage companies to adopt voluntary security standards and direct federal agencies to determine whether existing cyber security regulations are adequate.

The president's de facto re-routing of all Internet traffic through federal intelligence officers deputizes more than just DHS as cybertraffic cops. The AP reports that "the Pentagon, the National Security Agency (NSA), the director of national intelligence, and the Justice Department" will all cooperate in the surveillance — in the name of national security, of course.

Corporate employees will be authorized to snoop, as well. Per the AP's reading of the draft executive order, "selected employees at critical infrastructure companies would receive security clearances allowing them to receive the information."

As for those companies considered less critical to our national cybersecurity, "the government would ask businesses to tell the government about cyberthreats or cyberattacks. There would be no requirement to do so."

Given the history of the federal government's penchant for vague language, however, it is likely that despite the denial of compulsory cooperation with the government, there will be a loophole just large enough to mandate private cooperation with the federal government.

Although the president and officials in his administration portray the attack as imminent, Congress isn't persuaded, and on several occasions lawmakers have rejected measures calling for greater government control over the Internet and the communications infrastructure.

As mentioned above, however, that legislative lassitude may be a thing of the past in light of recent electoral events. Perhaps GOP congressional leadership might see "protecting our nation's cybersecurity" as a politically safe expression of bipartisanship.

Regardless of any renewed spirit of cooperation, President Obama is unlikely to set his watch by Congress's timetable. The president, in fact, has been anxious to seize control of the Internet since his inauguration in 2009. As *The New American* reported that year:

> The president pointed out that shortly after taking office he directed the National Security Council and Homeland Security Council to thoroughly review the federal government's efforts "to defend our information and communications infrastructure" and to recommend improvements. He mentioned that National Security Council Acting Senior Director for Cyberspace Melissa Hathaway led the review team, and that the 60-day review included input from industry, academia, civil liberty and privacy advocates, every level and branch of government, Congress, and other advisers — even input from "international partners."

To that end, the White House proposed legislation in 2011 and has ordered one after the other administration official to testify at no fewer than 17 congressional hearings on the subject.

In a recent *Wall Street Journal* opinion piece penned by the president, he did his best to instill in the American people fear of the consequences we would suffer should someone launch a successful

cyberattack on the critical infrastructure networks of our nation.

National Security Council spokesman Caitlin Hayden was quoted parroting the president's party line on the urgent need for action, however: "Given the gravity of the threats we face in cyberspace, we want to get this right in addition to getting it done swiftly," Hayden told the AP.

The same sense of urgency is being stirred up in other places around D.C. As described in an article published by FCW:

> Combined with the increasing public awareness of the cyber threat — and subsequent pressure on lawmakers to take action — the end of election season sets the stage for action on cybersecurity, according to a panel of insiders speaking Nov. 7 at the Symantec Government Symposium in Washington.
>
> "There's the trifecta of knowing who controls the Senate, knowing who the President is and the fact that there's not an election. That, combined with the executive order looming, has to change the calculation of the people, organizations and stakeholders that sought to and did obstruct legislation," said Clete Johnson, professional staff and counsel for the Senate Select Committee on Intelligence.

And:

> "I think it's difficult to put where on the scale [of legislative priorities] cybersecurity will be. I think both [Speaker of the House John Boehner] and [Senate Majority Leader Harry Reid] have the realization of how important this issue is, and certainly the White House does too," said Michael Seeds, legislative director for Rep. Mac Thornberry (R-Texas). Still, "anything with the word 'regulation' tied to it is going to be difficult to get through the House. I'm not sure how much of that has changed since the election or under the threat of the executive order. I do think a lot of the work we've done over the past year is laying the groundwork for continuing the conversation into the next Congress.

That pace probably isn't fast enough for a president with a full tank of gas and a lead foot. The announcement of a cybersecurity executive order with all the necessary protections for safety and the requisite disregard for constitutional separation of powers is probably more imminent than we think.

Despite the uncertainty of the timetable, what is certain is that once President Obama signs his name to that edict and assuming compliance with its mandates changes from voluntary to involuntary, he will possess powers only dreamed about by the most ambitious dictators of history.

Photo: AP Images