Written by **Joe Wolverton, II, J.D.** on October 24, 2012

Obama Closer to Seizing Control of Cyberspace; Exec. Order Imminent

According to a copy of a draft executive order on cybersecurity obtained by the Associated Press (AP), President Obama will soon order "U.S. spy agencies to share the latest intelligence about cyberthreats with companies operating electric grids, water plants, railroads and other vital industries to help protect them from electronic attacks."

For some time, government officials have insisted that Iran is planning a cyberattack on the electronic communications infrastructure of the United States. The AP reports that Defense Secretary Leon Panetta said that the U.S. armed forces are "ready to retaliate" should Iran — or any other country — attempt an attack on U.S. cybersecurity.

Promises of the White House's imminent issuing of the edict have been coming for months. The AP reports that regardless of the latest leak, "the White House declined to say when the president will sign the order."

On September 19, 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.

The president claims that this legislative lassitude is forcing him to bypass the Constitution and act alone to protect the country from cyberattacks. Once Barack Obama signs his name to this 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.

"In the wake of Congressional inaction and Republican stall tactics, unfortunately, we will continue to be hamstrung by outdated and inadequate statutory authorities that the legislation would have fixed. Moving forward, the President is determined to do absolutely everything we can to better protect our nation against today's cyber threats and we will do that," White House Press Secretary Jay Carney said in an email reported by *The Hill*.

The demise of the bill in the Senate was not unforeseen. As *The New American* reported in July:

> The Cybersecurity Act of 2012 has been the subject of some criticism as privacy advocates feared that the bill would pose too many threats to the constitutional rights of the American people.
>
> Likewise, the U.S. Chamber of Commerce and IBM sent out letters to show their opposition for the original bill, asserting that it would overwhelm the industry with regulations.
>
> In response to the criticism, Senator Lieberman reformed the original bill.
>
> For example, the updated version of the bill reflects changes to the provision to assign the Department of Homeland Security the role of creating mandatory cybersecurity standards for infrastructure industries.
>
> The newer version of the bill does not include language for "mandatory, regulatory sections," but still requires a creation of industry best practice standards for the purposes of protecting critical infrastructure, but rather than making the adoption of those standards mandatory, the owners of

> the critical infrastructure adopt "voluntary" standards. The bill offers incentives to adopt those standards, such as liability protection, and access to threat information.
>
> Some contend that the revisions are not ideal, however, as it gives the government the power to deny threat information to critical infrastructure owners who choose not to comply with the voluntary standards. Likewise, the incentives are too insignificant to fully incentivize any company to adopt the standards.

Since the beginning of his administration, President Obama has made cybersecurity a central plank in his presidential platform. As *The New American* reported in 2009:

> 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.

The AP reports that the version of the order it obtained was undated and that Obama administration spokesmen refused to disclose when President Obama would issue the order.

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.

Photo of President Barack Obama: AP Images