Obama's exec order draft on cybersecurity stirs debate

Bill's backers, civil liberties groups, business and security community all have views on the matter. Here's a sampling

By Taylor Armerding September 14, 2012

President Obama's draft of an Executive Order (EO) to implement some of the provisions of the 2012 Cyber Security Act (CSA), which failed in the U.S. Senate earlier this month, has reignited the debate over government's role in cybersecurity

The Hill reported last week that the draft is circulating among federal agencies for feedback, and *RT* reported Wednesday that the White House had leaked a copy of the draft to Associated Press.

Multiple reports said one of the key elements of the draft is that it will establish a cybersecurity council chaired by the Department of Homeland Security (DHS), which will develop a report to determine which agencies should regulate which parts of the nation's "critical infrastructure."

Other provisions are that it would require government information sharing about threats, create voluntary standards for critical infrastructure industries, strengthen oversight of cybersecurity by regulatory agencies, and use federal procurement as a means of pressuring companies to improve security.

On one side of the debate are advocates of the impending EO, including Sens. Dianne Feinstein (D-Calif.) and Jay Rockefeller (D-WVa.), who each wrote letters to President Obama recently, urging him to issue an EO, saying securing the nation's vital infrastructure from cyberattack is too important to wait for action from a gridlocked Congress.

[See also: Private sector fights on despite cybersecurity bill's failure]

On the other side are business and civil liberties groups who contend that the president is wrong to circumvent Congress, that the order will be too costly, too

heavy handed, ineffective and is not even necessary, since the private sector is finally addressing cybersecurity aggressively on its own.

There is a range of opinion within the security community as well, on the following major issues raised by critics:

The president should not circumvent Congress on a matter of this importance:

Some, like Kurt Nimmo, writing on *Infowars.com*, contend that,"Obama plans to violate the Constitution again."

Jacob Olcott, principal at Good Harbor Consulting, considers that a vast overstatement. "The executive branch creates policy every day without congressional input," he said. "They adopt executive orders all the time. It's not a constitutional crisis -- it's the way our government works."

Others fall somewhere between those views. Randy Sabett, an attorney with ZwillGen and a specialist in information security, doesn't consider it a constitutional issue, but said, "the legislative process is there for a reason. The more this (EOs) happens, the more problematic it becomes because you don't have input from all sources, which is the basis of our government."

Sabett said legislation can be a, "long, painful, deliberative process," but that it is meant to include all views and voices. "With an executive order, you end up shutting out those voices," he said.

Jody Westby, CEO of Global Cyber Risk and an attorney, writing in *Forbes* magazine, expressed similar concern. "Wow. If Democratic Senators cannot get a bill passed in the legislative chamber that they control, they will see if the executive branch can do their work for them," she wrote. "Gee, that even saves them having to wrangle through a conference with the House."

Roger Thornton, CTO of AlienVault, said the intent, to compel private industry to protect critical infrastructure, is laudable. "A mandate backed by Congress and the president would probably be more effective at convincing the private sector," he said. "It seems to me that if the president and congress are disagreeing, they will have a hard time leading the private sector to a solution of any kind."

It would give the DHS cybersecurity council too much power to determine what is critical infrastructure:

Jim Harper, director of information policy studies at the Cato Institute, warned this week in *United Liberty* to, "Keep an eye on that phrase, 'critical infrastructure,' because it's a notorious weasel-word."

Harper said he had argued before Congress in 2009 that something should be considered critical if, "compromise of the resource would immediately and proximately endanger life and health."

But he said a report by the Center for Strategic and International Studies (CSIS) said, "'[Critical] means that, if the function or service is disrupted, there is immediate and serious damage to key national functions such as U.S. military capabilities or economic performance.'

"When hungry bureaucrats are doing the interpreting, economic performance means 'anything,'" Harper wrote.

Randy Sabett agrees, adding that companies marked as critical, "won't even have a process to appeal it. If you went through legislative process to determine what is critical infrastructure, that would be one thing. But to have DHS defining this phrase, there's a significant risk that they're going to get it wrong," he said.

While compliance with standards is being called "voluntary," it will in fact be mandatory:

James Lewis, director of the technology and public policy program at CSIS, told The Hill that the program simply won't work if it is truly voluntary, largely because of what he called a "spotty track record" by DHS in leading national security efforts.

"Find me a company that says 'I'm going to voluntarily agree to be regulated by DHS.' Nobody is going to volunteer to have DHS regulate them," Lewis said.

Joel Harding, a retired military intelligence officer and information operations expert, agrees that mandatory is necesary. "Anything written as voluntary will be, de facto, mandatory," he said. "For the system to work, protecting our companies and corporations, the vast majority must cooperate. Without a large percentage of businesses submitting their data, the overall situational awareness will not be accurate."

It would burden businesses with regulations that would be costly, and not make them any more secure:

Steven Bucci, in a blog post on the Heritage Foundation's *The Foundry*, wrote that, "(Regulation) is exactly the wrong approach for dealing with a fast-moving and incredibly dynamic field like cybersecurity. Give hackers - whether working for themselves or for another nation-state -- a static standard, and they will waltz around it and have their way with the target entity."

Randy Sabett said this is his major area of concern. "I'm less concerned about voluntary vs. mandatory, and more about what is effective from security

perspective," he said, adding that compliance with regulations does not always yield better security.

"A lot of agencies have spent a lot to comply with FISMA (Federal Information Security Management Act). You can check the boxes, but when the security report card comes out and you have agencies with a D- that are still getting funding, what does that tell us?"

Sabett said in government, if an agency is not meeting standards, it simply gets more money to help it comply. "But in the commercial sector, you don't have this easy flow of money if you're not doing well," he said. "You wind up paying money for something that is going to be ineffective."

Joel Harding said he believes regulatory pressure from government is still necessary.

An EO is not necessary, since the private sector is addressing this on its own:

"Without the reporting that will be required, incidents, including intrusions, exploitation and intellectual property theft, will continue to grow rampantly. By not reporting, by not having regulation, the businesses hurt themselves in the long run," he said.

But Westby told *CSO Online*: "Businesses don't like regulations; An executive order will pit the business community against government, which is counterproductive to improving cybersecurity. Regulations will hardly incentivize businesses to take action on cybersecurity. It will put them in the position of only doing what they have to do to meet compliance requirements."

An EO is not necessary, because businesses are addressing security on their own:

Richard Stiennon, writing in Forbes, argued that, "The good news is that while Congress dithered, the IT security industry developed.

"Threat based cyber security is the fastest growing sector in the IT security industry. The rapid uptake represented by 100% annual growth rates indicated that without a single regulation or Executive Order the problem is being addressed," he wrote, adding that imposing regulations on infrastructure operators, "based on outmoded asset and vulnerability methodologies will distract them from implementing threat based defenses. The draft Executive Order, if issued, will do much more harm than good."

But Sabett counters that while the private sector does have an interest in its own security, they still need a "nudge" from government. He said in 2003 that former

Florida Congressman Adam Putnam proposed a bill that was "sort of like Sarbanes-Oxley for cybersecurity. And business went crazy. Everybody said, 'We'll take care of it.'"

"But here were are in 2012 and things haven't gotten much better."