The Washington Times

Administration's cybersecurity directive inadequate for industry, analysts say

By Shaun Waterman – February 13, 2013

Cybersecurity analysts on Wednesday criticized the Obama's administration's new plan to protect vital industries such as banking and energy from attacks by hackers, spies and foreign enemies.

Several analysts said that legislation is still needed to authorize federal agencies to regulate cybersecurity standards in the private sector, even after the presidential directive and executive order that Mr. Obama signed Tuesday.

Libertarians and business interests fretted about the possibility that the voluntary computer-security standards the orders promote might grow into a quasi-regulatory framework that stifles in red tape the companies that own critical industries.

"The danger is that this could easily grow into the centralized, bloated micromanagement of private-sector network security," Julian Sanchez, a research fellow at the libertarian Cato Institute, told The Washington Times.

Mr. Sanchez said he is especially troubled that the orders give so much authority to the Department of Homeland Security to manage voluntary standards and public-private partnerships designed to protect U.S. industrial computer systems from attack via the Internet.

"The culture [at Homeland Security] does not seem to be one where employees are encouraged to recognize the limitations of their own expertise," Mr. Sanchez said.

He noted that a congressional report last year found that Homeland Security officials continued to give glowing progress reports to lawmakers on the department's nationwide network of counterterrorism "fusion centers" even when internal audits had revealed serious weaknesses in how they worked.

Rep. Mike Rogers, chairman of the House Permanent Select Committee on Intelligence, said Wednesday that Congress needs to "fill in the gaps" left by the president's orders by providing legal protections for companies that cooperate with the government on cybersecurity.

"We are in a cyberwar already, and most Americans don't know it," the Michigan Republican said. "And at this point, we're losing."

Mr. Rogers said that hackers have attacked the websites of a growing number of U.S. banks since last fall, when Congress failed to pass any of several cybersecurity bills.

The attacks have not compromised bank accounts or financial data, but have prevented customers logging on for hours at a time and sometimes made online access difficult for several days.

The hackers, who announce their targets in advance online, call themselves "The Cutting Sword of Justice" and say they are Muslims outraged by a U.S.-made video that disparages Islam's Prophet Muhammad.

But Mr. Rogers said Iran is behind the hacking, which he said looks like "probing" attacks that an enemy undertakes to test a nation's defenses.

The president's plan aims to provide more secret intelligence about cyberthreats, especially from spies and hackers, to the private sector, which owns more than 80 percent of the infrastructure vital to Americans' everyday lives — from banking and telecommunications services to water systems, hospitals and transit networks.

"We know hackers steal people's identities and infiltrate private emails. We know foreign countries and companies swipe our corporate secrets," Mr. Obama said Tuesday in his State of the Union address. "Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air-traffic control systems."

The presidential directive and executive order give government scientists and officials a year to devise a "baseline framework" — a term critics deride as vague — for cybersecurity incorporating "consensus standards and industry best practice" on how to secure computer networks.

The standards will be voluntary, except where government agencies can use regulatory authority to enforce them.

A senior administration official who briefed reporters Tuesday said that many industrial sectors, such as energy, already are "moving aggressively" to adopt best practices in cybersecurity.

The regulatory review the president has ordered "is really a backstop to what we think will already be happening in the marketplace," the official said.

"They are trying to be flexible in their approach, recognizing that each sector is very different," said Jessica Herrera-Flanigan, a government-affairs consultant in cybersecurity.

For example, telecommunications systems generally are owned by large high-tech companies whose staff include the best cybersecurity expertise available. By contrast, many water systems in rural or small communities are "mom and pop" operations without even an in-house tech staff.

Making rules that make sense for operations as diverse as global phone companies and rural water utilities is one of the challenges of securing vital computer systems, analysts say.

The presidential orders "are specifically designed not to be a one-size-fits-all approach," said a senior administration official, noting that each sector is overseen by an agency.