# Obama Push

**Obama Pushing Now**

**Obama, 7/20** – President of the United States (Barack, “Taking the Cyberattack Threat Seriously”, 7/20/12, Wall Street Journal, [http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html)//GP](http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html%29/GP)

This is exactly the kind of responsible, collaborative approach to an urgent national-security challenge that Americans expect but that Washington too rarely provides. It reflects the insights and ideas of industry and civil libertarians. **It is sponsored by a bipartisan group of senators**. It is supported by current and former homeland security, intelligence and defense leaders **from both Republican and Democratic administrations**.

Today we can see the cyber threat to the networks upon which so much of our modern American lives depend. We have the opportunity—and the responsibility—**to take action now** and stay a step ahead of our adversaries. For the sake of our national and economic security, I urge the Senate to pass the Cybersecurity Act of 2012 and Congress to send me comprehensive legislation so I can sign it into law.

It's time to strengthen our defenses against this growing danger.

**Cybersecurity is Obama’s top priority**

**Poremba 7/27** - a writer in addition to covering IT security topics for IT Business Edge and Network Security Edge, she reports on security alerts and vulnerabilities, as well as common-sense measures to keep your data  (Sue, “What Congress' cybersecurity bills mean for you” NBC News, 7/27/12

 <http://today.msnbc.msn.com/id/48351359/ns/today-today_tech/t/what-congress-cybersecurity-bills-mean-you/>)//GP

President Barack Obama is currently pushing for cybersecurity legislation and **has made it one of his priorities for 2012.**

In a [July 19 opinion piece](http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html)published in The Wall Street Journal, the president wrote, "It doesn't take much to imagine the consequences of a successful cyber attack. In a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home.

"This is the future we have to avoid," he wrote. "**That's why my administration has made cybersecurity a priority,** including proposing legislation to strengthen our nation's digital defenses. It's why Congress must pass comprehensive [cybersecurity](http://www.securitynewsdaily.com/438-white-house-america-needs-a-new-cybersecurity-force.html) legislation."

Congress hasn't ignored the call. Members of both the House and Senate have introduced a number of bills in recent months, most of which are being hashed out in committees.

As of this writing in late July, one piece of legislation**, the Cybersecurity Act of 2012, is expected to be brought up for debate on the Senate floor in a matter of days.**

According to Dan Stickel, CEO of Metaforic, a software-security company in San Jose, Calif., there are two primary categories into which the approximately 30 bills that have been introduced fall: data-breach tracking and [infrastructure hardening](http://www.securitynewsdaily.com/1529-cybersecurity-bill-critical-infrastructure.html).

[Data-breach](http://www.securitynewsdaily.com/1959-data-breach-definition.html)tracking is meant to thwart the [theft of sensitive information](http://www.securitynewsdaily.com/1675-chinese-cybercrime-traced-man.html), such as when outsiders break into systems and steal consumers' Social Security numbers or companies' secret design plans.

"Mostly, the government is trying to provide a clearinghouse of information so people can track what's going on, how people are getting attacked, etc., and try to shore up the defenses," Stickel said. "These breaches are a real problem, and costly, but we're living with them."

Infrastructure hardening is part of an effort to protect the country's critical infrastructure, such as power plants and water supplies, from an attack by a foreign power, a terrorist organization or even organized crime.

Such attacks are rare — many experts argue they've never even taken place — but the [weaknesses in critical-infrastructure data security](http://www.securitynewsdaily.com/685-critical-flaw-leaves-oil-refineries-open-to-cyberattack.html)make possible an attack that could cripple large regions of the nation.

# I/L !

**Cyber Security Infrastructure is vulnerable to terrorists now**
**Peterson, 7/20** - Tech Editor at The Daily Caller Past: Social Media Editor at Meet Mrs. B, Scribe Investigative Reporter at The Heritage Foundation, MMA Contributor at Bleacher Report, Reporter/Nation, Heritage Foundation CAIR Workshop, Leadership Institute, Hillsdale College Summary Tech Editor for The Daily Caller. Peterson is a DC-based technology and investigative reporter, covering the intersection of...

 (Josh, [“Obama scares the hell out of everybody with cybersecurity op-ed](http://dailycaller.com/2012/07/20/obama-scares-the-hell-out-of-everybody-with-cybersecurity-op-ed/)”, 07/20/2012, The Daily Caller, http://dailycaller.com/2012/07/20/obama-scares-the-hell-out-of-everybody-with-cybersecurity-op-ed/#ixzz222OWMLEt)//GP

In a Thursday Wall Street Journal Opinion piece, President Barack Obama evoked images of mass disaster should a cyber attack wreak havoc on the nation’s transportation and water systems.

**Fear of a deadly cyber-attack by a state or terrorist group loom heavy over the heads of lawmakers**, as well as current and former high-ranking national security officials. Obama’s piece echoed a consistent theme: The nation’s cyberdefenses **are vulnerable to major attack from states and terrorists**, and federal legislation must be passed that would require companies that are part of the nation’s critical infrastructure to abide by federal safety standards.

If the alleged leaks about the U.S. cyberwarfare program are true, then the U.S. has already demonstrated that such capabilities are within reach. The famed STUXNET virus, which caused centrifuges used for enriching uranium at a secret Iranian nuclear facility to malfunction, was targeting Iranian progress towards developing a nuclear weapon.

**Tension between the U.S. and China over cyber security now**

**Osnos, 7/25** -  an American reporter for The New Yorker, based in Beijing. Previously, he was an international correspondent for The Chicago Tribune in Beijing. Before that, he covered the Iraq War for that newspaper.  (Evan, “Q. & A.: The Cybersecurity Bill, China, and Innovation” 7/25/12, The New York Times, http://www.newyorker.com/online/blogs/evanosnos/2012/07/adam-segal-on-cybersecurity-china-and-innovation.html#ixzz222NjIKW4)//GP

Cyber is often mentioned as one of the leading potential flashpoints in the U.S.-China relationship. Where would you rank that risk compared to potential conflict in the South China Sea, Taiwan, or trade disputes?

While strategic mistrust is high between the two sides, Cyber alone is unlikely to be a major flashpoint. Attacks designed to steal intellectual property and other trade secrets occur with such regularity and at such a pace and scope that General Alexander, head of U.S. Cyber Command, has called them “the greatest transfer of wealth in history”—yet the United States continues to engage China on a range of issues, from Iran and Syria to trade and the environment. Washington has raised the pressure on Beijing about cyber, publicly calling out Chinese hackers and addressing it in bilateral meetings, but clearly has not made it an issue that it is willing to go to the mat for.

There is little doubt, however, that cyber will be part of any political, military, or economic conflict in the future, and that it has high a probability of making the situation more difficult to resolve. Web-site defacements were an annoyance in the standoff between China and the Philippines over the Scarborough Shoal/Huangyan Island, but more serious cyber attacks could have escalated the situation, making signalling much more complicated. This is why it is so important that the United States and China continue to talk about cyber and to **develop points of contact and other communication mechanisms in case of crisis.**

# Impacts

**Laundry List of Impacts – financial crisis, blackouts, lack of clean water, and terrorist attacks**

**Obama, 7/20** – President of the United States (Barack, “Taking the Cyberattack Threat Seriously”, 7/20/12, Wall Street Journal, [http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html)//GP](http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html%29/GP)

In a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home.

Last month I convened an emergency meeting of my cabinet and top homeland security, intelligence and defense officials. Across the country trains had derailed, including one carrying industrial chemicals that exploded into a toxic cloud. Water treatment plants in several states had shut down, contaminating drinking water and causing Americans to fall ill.

Our nation, it appeared, was under cyber attack. Unknown hackers, perhaps a world away, had inserted malicious software into the computer networks of private-sector companies that operate most of our transportation, water and other critical infrastructure systems.

Fortunately, last month's scenario was just a simulation—an exercise to test how well federal, state and local governments and the private sector can work together in a crisis. But it was a sobering reminder that **the cyber threat to our nation is one of the most serious economic and national security challenges we face.**

So far, no one has managed to seriously damage or disrupt our critical infrastructure networks. But foreign governments, criminal syndicates and lone individuals are probing our financial, energy and public safety systems every day. Last year, a water plant in Texas disconnected its control system from the Internet after a hacker posted pictures of the facility's internal controls. More recently, hackers penetrated the networks of companies that operate our natural-gas pipelines. Computer systems in critical sectors of our economy—including the nuclear and chemical industries—are being increasingly targeted.

It doesn't take much to imagine the consequences of a successful cyber attack. In a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home. Taking down vital banking systems could trigger **a financial crisis**. The **lack of clean water** or functioning hospitals could spark a **public health emergency**. And as we've seen in **past blackouts**, the loss of electricity can bring businesses, cities and **entire regions to a standstill**.

This is the future we have to avoid. That's why my administration has made cybersecurity a priority, including proposing legislation to strengthen our nation's digital defenses. **It's why Congress must pass comprehensive cybersecurity legislation.**

We all know what needs to happen. We need to make it easier for the government to share threat information so critical-infrastructure companies are better prepared. We need to make it easier for these companies—with reasonable liability protection—to share data and information with government when they're attacked. And we need to make it easier for government, if asked, to help these companies prevent and recover from attacks.

Yet simply sharing more information is not enough. Ultimately, this is about security gaps that have to be filled. To their credit, many of these companies have boosted their cyber defenses. But many others have not, with some lacking even the most basic protection: a good password. That puts public safety and our national security at risk.

The American people deserve to know that companies running our critical infrastructure meet basic, commonsense cybersecurity standards, just as they already meet other security requirements. **Nuclear power plants must have fences and defenses to thwart a terrorist attack.** Water treatment plants must test their water regularly for contaminants. Airplanes must have secure cockpit doors. We all understand the need for these kinds of physical security measures. It would be the height of irresponsibility to leave a digital backdoor wide open to our cyber adversaries.

**The terrorist threat is dire – makes us vulnerable and risks national security**

**Clabough, 7/25** - Writer at The New American, Adjunct Professor at [Hillsborough Community College](http://www.linkedin.com/company/hillsborough-community-college?trk=ppro_cprof), studied at the State University of New York at Albany (Raven, “Senate to Consider Cybersecurity Act of 2012”, The New American, 7/25/12, <http://www.thenewamerican.com/usnews/politics/item/12211-senate-to-consider-cybersecurity-act-of-2012>)//GP

"The threat is extremely dire,” Lieberman said. “I am literally worried that an attack could be **imminent**. We know that both states, countries like China, Russia and Iran are constantly probing our cyber networks, both government and private, and both civilian and defense.
"We know that countries and terrorist groups and organized crime groups are constantly trying to steal industrial secrets form American companies that they’ve invested millions in, sometimes billions in, to basically get it for nothing and then create those industries and jobs over in other countries."

Citing remarks made by Secretary of Defense Leon Panetta and National Security Agency head General Keith Alexander on the imminence of a cyber attack and the destruction it would cause, Lieberman said, “We’re very vulnerable to attack and some of the private owners of critical cyber infrastructure, like the electric grid or the financial system, banking systems, transportation, water.”

“Some of them are doing a pretty good job at defending their cyberspace, but some are not, and the main aim of this bill is to make sure that the private owners — 85 percent of our infrastructure … are taking steps to defend the cyberspace they own because that may well represent defense of our country."

Meanwhile, Republicans have threatened to delay consideration on the cyber security bill until the Senate takes up legislation on defense authorization.

Senate Majority Leader Harry Reid responded to such a threat by asserting, “Failing to act on cyber security legislation not only puts our national security at risk,” but also “recklessly endangers members of our armed forces and missions around the world.”

# Will Pass

**Will Pass now – Obama push and bipartisan support**
**Peterson, 7/20** - Tech Editor at The Daily Caller Past: Social Media Editor at Meet Mrs. B, Scribe Investigative Reporter at The Heritage Foundation, MMA Contributor at Bleacher Report, Reporter/Nation, Heritage Foundation CAIR Workshop, Leadership Institute, Hillsdale College Summary Tech Editor for The Daily Caller. Peterson is a DC-based technology and investigative reporter, covering the intersection of...

 (Josh, [“Obama scares the hell out of everybody with cybersecurity op-ed](http://dailycaller.com/2012/07/20/obama-scares-the-hell-out-of-everybody-with-cybersecurity-op-ed/)”, 07/20/2012, The Daily Caller, http://dailycaller.com/2012/07/20/obama-scares-the-hell-out-of-everybody-with-cybersecurity-op-ed/#ixzz222OWMLEt)//GP

**The president threw his weight behind the Cybersecurity Act of 2012**, which is sponsored by Independent Connecticut Sen. Joe Lieberman and Maine Republican Sen. Susan Collins, and favored by Democratic Sen. Majority Leader Harry Reid.

After it was introduced in February, the bill was [opposed](http://dailycaller.com/2012/02/06/democrats-to-continue-internet-coup-with-new-cyber-bill/) by Senate Republicans and the U.S. Chamber of Commerce for giving the Department of Homeland Security the ability to assess and set the security standards for power companies, utilities and other companies considered part of the nation’s critical infrastructure.

In order for the bill to make it through the Senate, however, Reid will need the support of his Republican colleagues. Lieberman and several of his colleagues [reintroduced](http://arstechnica.com/tech-policy/2012/07/senate-introduces-revised-version-of-the-cybersecurity-act-of-2012/) a revised version of the bill on Thursday that is **designed to meet Republican concerns** — particularly that government and the private sector should share threat information in order to bolster defenses against incoming attacks.

The revision also attempts to appease critics of the Cyber Intelligence Sharing and Protection Act — a bill that won favor in the Republican-controlled House of Representatives for its emphasis on information-sharing between the federal government and the private sector. Critics of the bill feared that such information-sharing provisions would violate civil liberties and privacy. The revisions seek to address those concerns as well.

While lawmakers push to pass legislation before November, **the bill could see a floor vote as early as next week to make it in time before the August recess.**

“So far, no one has managed to seriously damage or disrupt our critical infrastructure networks,” Obama wrote. “But foreign governments, criminal syndicates and lone individuals are probing our financial, energy and public safety systems every day.”

**Will pass – compromise measures have been taken for the GOP to come on board**

**Fitzpatrick, 7/26** - a Reporter at Mashable's New York headquarters, where he covers the intersection of politics, international affairs, social media and technology. He initially joined Mashable as a Community Intern in October of 2011. (Alex, “[Cybersecurity Bill Inches Closer to Passing](http://mashable.com/2012/07/26/cybersecurity-bill-senate/)”, Mashable, 7/26/12, <http://mashable.com/2012/07/26/cybersecurity-bill-senate/>)//GP

The Lieberman-Collins cybersecurity bill moved one step closer to passing Thursday afternoon. The Senate voted in favor of a motion to proceed 84-11 after a lengthy and contentious debate. The bill now faces additional changes before being brought up for a full vote.

The Cybersecurity Act, or CSA, is the Senate’s attempt to address cybersecurity reform. Senate leadership considers such reform a priority for the current term that ends in January.

As written, the CSA would set up an optional program where businesses deemed critical to the national infrastructure (such as power grids) would be asked to meet cybersecurity standards set by a group of government agencies. It would also establish a protocol for government agencies and businesses to share cybersecurity threat information with one another.

The bill originally called for government-mandated cybersecurity standards for key infrastructure with no opt-out. Senate Rebublicans considered that to be an example of excessive regulation. The opt-in compromise was **the key factor** in reducing Republican opposition.