



Myth vs. Fact: The Cybersecurity Act of 2012

The threat to America's computer networks and the critical infrastructure they operate is grave and growing. The Cybersecurity Act of 2012 is crafted to address this emerging threat with a balanced, cooperative, and business-friendly approach that ensures strong partnership between the government and private sector. Instead of working together to combat the threat, opponents of the bill continue to distort the truth by making false charges about the legislation's impact on the economy and individual freedoms.

Myth - The Cybersecurity Act will kill jobs.

Fact – Enhanced cybersecurity protects jobs by preventing cyberattacks that sap our economy.

- **Foreign competitors like China are stealing intellectual property from American businesses.** A recent unclassified report by the National Counterintelligence Executive described a persistent, widespread campaign by foreign nation-states to steal intellectual property and trade secrets from American companies. “Chinese actors,” it found, “are the world’s most active and persistent perpetrators of economic espionage.” It is estimated that American companies lose roughly \$250 billion a year to intellectual property theft, and former Secretary of Commerce John Bryson has noted that, “cyber espionage means fewer American jobs.” [[NCIX report to Congress](#), 10/11; Former U.S. Secretary of Commerce John Bryson, [Politico](#), 3/8/12; [Foreign Policy](#), 7/9/12]
- **Cyber incidents cost consumers billions of dollars every year.** A recent study conducted by Norton, an Internet security company, estimates that during a year cybercrimes - including identity theft and online scams - cost the U.S. \$140 billion in cash and lost time. It found the \$388 billion global cost of cybercrime to be greater than the black market for marijuana, cocaine, and heroin combined. [[Symantec](#), 9/7/11; [Symantec](#)]
- **The Cybersecurity Act protects and creates jobs.** The Cybersecurity Act addresses the need for more computer science programs in high schools and universities to develop educated and skilled leaders and innovators in the field. By cultivating future generations of tech-savvy Americans and investing in development of a highly-skilled cyber workforce, the act would create jobs and help the U.S. maintain its global leadership in technology industries.

- **The Cybersecurity Act will spur innovation by enhancing research and development of cyber defense technologies.** The legislation would strengthen the nation's cyber defenses through research and development initiatives to build innovative security technologies. Developing incentives to secure the Internet would create demand for cutting edge products to stay ahead of evolving threats, and would drive further advancement in the field. As a result, security will increase nationwide and American innovators will reap the benefits.

Myth - The Cybersecurity Act imposes burdensome regulations on businesses.

Fact – Cybersecurity measures are voluntary, and create a strong public-private partnership to prevent cyberthreats.

- **The security framework would be voluntary.** The Cybersecurity Act will establish a partnership between government and industry to prevent cyberattacks. A National Cybersecurity Council – led by the Department of Homeland Security and comprised of representatives from federal agencies, state and local governments, and business – would create outcome-based performance standards. Compliance would be completely voluntary. Incentives to voluntarily adopt these standards would include liability protection in the event of an attack, expedited security clearances to facilitate information sharing, and priority cyber assistance from the government.
- **The security framework targets only the most critical infrastructure.** The National Cybersecurity Council will identify specific critical infrastructure computer networks that if attacked, would lead to mass casualties, cripple the economy, or degrade the country's national security. These could include major utilities or financial networks. The overwhelming majority of personal, private, and small business systems would not be impacted.
- **Critical infrastructure operators would have the flexibility to develop security methods that best fit their needs.** Critical infrastructure operators that choose to meet voluntary standards would be free to do so in any way they deem appropriate. The approach would be outcome-based, meaning it would not matter *how* a critical infrastructure entity decides to secure its systems, only that the systems achieve the level of security identified by the Council. This voluntary approach provides flexibility for operators to secure computer systems without dictating specific technologies or processes.
- **The Cybersecurity Act does not allow federal agencies to circumvent existing regulators.** The legislation does not provide any new regulatory authority or any avenue for agencies to overstep existing authorities to regulate the private sector, and explicitly states, "Nothing...shall be construed to provide a Federal agency with authority for regulating the security of critical cyber infrastructure in addition or to a greater extent than the authority the Federal agency has under other law." An agency cannot bypass its existing security regulator. If a federal agency currently does not have the ability to craft its own regulations, but instead relies on a third party, that partnership will remain unchanged. [Section 103-G-1(C) of S.3414]

Myth - The private sector is better equipped to handle cybersecurity.

Fact – We need a coordinated partnership to counter cyberthreats.

- **Cyberattacks are a dangerous national security threat.** The Department of Defense (DoD) is probed millions of times a day by malicious cyber actors. By September 2011, DoD had identified over 70 million cumulative malware threats against its networks. In the last few years alone, malicious actors have launched cyberattacks against America's nuclear infrastructure, advanced military weapons systems, water treatment facilities, credit card companies, financial institutions and the NASDAQ stock exchange. [[Testimony of Assistant Secretary Zachary Lemnios](#), 3/20/12; [DoD Strategy for Operating in Cyberspace](#), 7/11]
- **National security is a government responsibility.** Malicious cyberattacks are among the most urgent threats to our country, and our national security demands a clear role for the federal government in developing cybersecurity standards. No other area of national security is left to private efforts. Attacks on major financial institutions and companies have demonstrated that private security is not enough. The stakes are too high to rely on an ad-hoc approach. [[CSIS](#), 12/08; [DPCC](#), 7/30/12]
- **Government expertise, technologies, and authorities outpace the private sector's ability to defend against cyberattacks.** The National Security Agency and U.S. Cyber Command operate and monitor all of the U.S. military's cyber activities. The Department of Homeland Security is charged with securing all of the non-military networks operated by the government, while the Federal Bureau of Investigation is responsible for investigating crimes that occur within the cyber realm. These entities support each other by sharing information and technical assistance, and together they possess unparalleled expertise, tools and abilities that strengthen America's cyber infrastructure far better than a patchwork of private sector initiatives could.

Myth - The Cybersecurity Act does not protect individual privacy.

Fact – Careful oversight and strong civil liberties protections are built into the bill.

- **Information can be shared without compromising individual privacy and civil liberties.** As General Keith Alexander, Director of the National Security Agency and U.S. Cyber Command, recently explained, "If the critical infrastructure community is being attacked by something, we need them to tell us -- at network speed. [But,] It doesn't require the government to read their mail or your mail to do that.... The reality is we can do protection of civil liberties and privacy and cybersecurity, as a nation. Not only we can.... we must." [[General Alexander's Remarks](#), 7/9/12; [AOL Defense](#), 7/9/12]
- **Only necessary threat information would be shared, while strong protections would safeguard privacy and civil liberties.** This legislation will protect Americans' privacy and civil liberties by strictly defining the information private entities may share with other private entities, by ensuring that such information may only be used for cybersecurity activities, and by ensuring that control of the information remains in civilian hands. This legislation prioritizes safeguarding any information that could expose personal communications or identities. These added protections ensure that the nation's cyber networks can be defended without compromising the freedom and anonymity of the internet.

Myth – Critical infrastructure should not be covered.

Fact – Critical infrastructure is vulnerable to cyberattacks that could have devastating consequences.

- **There has been a staggering increase in cyberattacks on critical infrastructure.** The number of cyberattacks on critical infrastructure reported to the Department of Homeland Security spiked from nine in 2009 to 198 in 2011. Similarly, a recent Symantec report documented an 81% increase in malware attacks in 2011 over 2010. The significant rise in attacks demonstrates the need for enhanced security and nationwide security standards across industries. [[CNN Security Clearance](#), 7/4/12; [Symantec](#), 4/12]
- **There is bipartisan consensus that critical infrastructure must be covered.** NSA Director General Keith Alexander recently wrote to Senator McCain, “Critical infrastructure protection needs to be addressed in any cyber security legislation. The risk is simply too great considering the reality of our interconnected and interdependent world.” Other notable advocates include: The co-chairmen of the 9/11 Commission, Governor Thomas Kean and Congressman Lee Hamilton; Director of National Intelligence, James Clapper; Director of the FBI, Robert Mueller; former Homeland Security Secretary under President Bush, Michael Chertoff; former Director of National Intelligence Mike McConnell; former Deputy Secretary of Defense Paul Wolfowitz; and former White House cybersecurity and counterterrorism advisor Richard Clarke. [[General Alexander’s letter to Senator McCain](#); [Testimony of Former Secretary Chertoff](#), 11/16/11; [Letters of Support](#)]