



United States Senate
Committee on Homeland Security and Governmental Affairs
Senator Joseph I. Lieberman, Chairman
Senator Susan M. Collins, Ranking Member

For Immediate Release
June 23, 2010

Contact: Leslie Phillips (Lieberman) 202-224-0384
Jeannine Guttman (Collins) 202-224-4751

Myth v. Reality
The Facts About S. 3480,
[“Protecting Cyberspace as a National Asset Act of 2010”](#)

WASHINGTON – Ahead of the Thursday, June 24, mark-up of this critical cybersecurity bill, Senators Joe Lieberman, ID-Conn, chairman of the Senate Homeland Security and Governmental Affairs Committee, and Susan Collins, R-Me., its Ranking Member, have issued the following fact sheet describing the intent and impact of their bipartisan legislation. This document also addresses some misconceptions about the bill:

FACTS:

The threat of a catastrophic cyber attack is real. It is not a matter of “if” an attack will happen; rather it is a matter of “when.” Just this March, the Senate’s Sergeant at Arms reported that the computer systems of the Executive Branch agencies and the Congress are now under cyber attack an average of 1.8 BILLION times per month.

Additionally, cyber crime costs our national economy billions of dollars annually. And, as intelligence officials have warned, malicious cyber activity occurs on a daily basis, on an unprecedented scale, and with extraordinary sophistication. As the former Director of National Intelligence Michael McConnell testified in February, “If we went to war today, in a cyber war, we would lose.”

MYTH #1:

S. 3480 authorizes a “kill switch” that would allow the President to shut down the Internet.

REALITY:

Rather than granting a “kill switch,” S. 3480 would make it far less likely for a President to use the broad authority he already has in current law to take over communications networks.

Section 706 of the *Communications Act of 1934* provides nearly unchecked authority to the President to “cause the closing of any facility or station for wire communication” and “authorize the use of control of any such facility or station” by the Federal government. Exercise of the authority requires no advance notification to Congress and can be authorized if the President proclaims that “a state or threat of war” exists. The authority can be exercised for up to six months after the “state or threat of war” has expired.

The Department of Homeland Security, in testimony before the Committee on June 15, 2010, indicated that Section 706 is one of the authorities the President would rely on if the nation were under a cyber attack.

S. 3480 would bring Presidential authority to respond to a major cyber attack into the 21st century by providing a precise, targeted, and focused way for the President to defend our most sensitive infrastructure.

- The authority in S. 3480 would be limited to 30-day increments and may be extended beyond 120 total days only with Congressional approval.
- The President *must use* the “least disruptive means feasible” to respond to the threat.
- The authority *does not* authorize the government to “take over” critical infrastructure.
- It does not authorize any new surveillance authorities.
- The President would be required to provide advance notice to Congress of the intent to declare a national cyber emergency or as soon as possible after a declaration, with reasons why advance notice was not possible.
- Owners/operators of covered critical infrastructure would be allowed to propose alternative security measures to respond to the national cyber emergency. Once approved by the Director of the National Center for Cybersecurity and Communications (NCCC), these security measures could be implemented instead of those previously required to respond to the cyber threat.
- Owner/operators that implement these emergency measures receive limited, civil liability protections for their actions.

MYTH #2:

S. 3480 would give the President the authority to take over the entire Internet.

REALITY:

S. 3480 would direct the President to set risk-based security performance requirements and, in a national cyber emergency, order emergency measures for our nation’s most critical infrastructure - those systems and assets that are most critical to our telecommunications networks, electric grid, financial system, and other components of critical infrastructure.

The bill authorizes only the identification of particular systems or assets – not whole companies, and certainly not the entire Internet. Only specific systems or assets whose disruption would cause a national or regional catastrophe would be subject to the bill’s mandatory security requirements.

To qualify as a national or regional catastrophe, the disruption of the system or asset would have to cause:

- mass casualties with an extraordinary number of fatalities;
- severe economic consequences;
- mass evacuations of prolonged duration; or
- severe degradation of national security capabilities, including intelligence and defense functions.

The bill expressly prohibits the Secretary from identifying systems or assets as covered critical infrastructure “based solely on activities protected by the first amendment of the United States Constitution.” This prohibition would also prevent the identification of specific websites for censorship.

The owners/operators of covered critical infrastructure identified by the Secretary could appeal the inclusion of the particular system or asset on the list through administrative procedures.

The list of covered critical infrastructure would be developed collaboratively, working with the private sector.

MYTH #3:

S. 3480 would give the President the authority to conduct electronic surveillance and monitor private networks.

REALITY:

This allegation is false. The bill creates no new authority to conduct electronic surveillance. It gives the government no new authority to compel the disclosure of private information. It does not alter the limitations of the *Wiretap Act*, the *Electronic Communications Privacy Act*, or the *Foreign Intelligence Surveillance Act*.

S. 3480 would establish a public/private partnership to secure cyberspace. It would encourage the private sector to voluntarily provide information about threats and vulnerabilities to our nation's information technology infrastructure.

Although owners/operators of covered critical infrastructure would be required to report on cyber attacks on their networks, the National Center for Cybersecurity and Communications (NCCC) would not have the authority to compel this disclosure.

Information provided to the NCCC by the private sector would be protected from unauthorized disclosure.

This system would rely on voluntary sharing of threat and vulnerability data and would help create a collaborative environment between the NCCC and the private sector.

MYTH #4:

S. 3480 would give the President the authority to regulate the Internet, which would limit innovation, impose costs on American businesses, and undermine competition, both at home and abroad.

REALITY:

The bill would set risk-based security performance requirements only for the owners/operators of our most critical systems and assets, which if disrupted would cost thousands of lives or billions of dollars in economic damage. The risk-based security performance requirements set by the NCCC would be developed in collaboration with the private sector.

Rather than setting specific standards, the NCCC would employ a risk-based approach to evaluating cyber risk. The owners/operators of covered critical infrastructure would develop a plan for protecting against those risks and mitigating the consequences of an attack. These owners/operators would be able to choose which security measures to implement to meet applicable risk-based security performance requirements.

This collaborative model would allow for continued innovation and dynamism that are fundamental to the success of the IT sector.

More fundamentally, the vast majority of this legislation embodies a public/private partnership to improve cyber security. Working cooperatively with the private sector, the NCCC would produce and share useful warning, analysis and threat information with the private sector. Furthermore, the NCCC would share information and work with the private sector to develop and promote best practices. The NCCC would provide voluntary technical assistance to the private sector to encourage adoption of best practices.

MYTH #5:

By including a strategy to ensure security is considered in federal information technology procurements, the bill would upset international standards for information technology products and services.

REALITY:

For too long, the federal government has failed to adequately account for security when procuring information technology products and services. S. 3480 would require the government to develop a strategy to consider security risks in information technology procurements. It would be similar to efforts already under way at the Departments of Defense and Homeland Security. This is simply a high level strategic effort that encourages collaboration by all stakeholders – it would not preclude particular businesses from contracting with the government.

The strategy would be developed by the Secretary of Homeland Security, in collaboration with all affected stakeholders – including the private sector. The strategy would be required to consider security based on risk, mission criticality, and cost effectiveness. The strategy would explicitly incorporate existing preferences for commercial-off-the-shelf products and services in Federal procurements.

The strategy would not circumvent or set aside international standards. Indeed, the bill would require the strategy developers to “place particular emphasis on the use of internationally-recognized standards and standards developed by the private sector.” If existing standards are not sufficient, the bill would direct the strategy to devise a process, working with the National Institute for Standards and Technology, to make recommendations for improvements to these standards.

To the extent necessary to implement the strategy, the FAR Council would incorporate portions of the strategy into the Federal Acquisition Regulations (FAR). These regulations would be the subject of public notice and comment under the well-established administrative process applicable to FAR changes.

These improvements in federal acquisition policy should have beneficial ripple effects in the larger commercial market. As a large customer, the federal government can contract with companies to innovate and improve the security of their IT services and products. With the government’s vast purchasing power, these innovations can establish new security baselines for services and products offered to the private sector and the general public. These improvements would develop by operation of the market and innovations among market competitors, not by regulation.

