The reading for this writing assignment is attached to this document as an article:

- **Senators propose granting president emergency Internet powers**
  - CNET News - June 10, 2010

Using the information from this article, answer the following questions:

1) Using the article and other sources (be sure to cite), briefly summarize the purpose of the bill titled: "Protecting Cyberspace as a National Asset Act of 2010", which is the subject of this article. In your summary, be sure to include what powers this bill is attempting to give the federal government. What is the current status of this bill?

2) One of the opponents of this bill, TechAmerica, said it was concerned about "unintended consequences that would result from the legislation's regulatory approach". What do you think some of the "unintended consequences" of this bill that they are referring to could be?

3) Joseph Lieberman has stated that "For all of its 'user-friendly' allure, the Internet can also be a dangerous place with electronic pipelines that run directly into everything from our personal bank accounts to key infrastructure to government and industrial secrets," he said. "Our economic security, national security and public safety are now all at risk from new kinds of enemies--cyber-warriors, cyber-spies, cyber-terrorists and cyber-criminals"

   - This course has made you experts in the field of Internet and Digital technology. Using what you know, do you think Lieberman's statement is completely true? Is it possible that he is exaggerating the risks of digital technology in an attempt to scare people into supporting the bill?

4) One of the key features of the Internet that we have discussed in this course is the fact that there is no central body that controls the Internet, meaning that the Internet is not policed by any one organization. If this bill passes, do you feel that this is an attempt by the United States government to have the NCCC control or police the internet?

5) To hand this assignment in, you will post it as a blog entry to your CSC101 Journal. The page we will be using for our journal from now on is entries.html, in your CSC101 folder. Consult your past lab reports, or the information found at w3schools if you are unsure of how to do this. Add a horizontal line between your last entry and this one, and also include the date the assignment is due under the horizontal line. Use any of the formatting tags that you know (or even some new ones) to make your entry look good.

   a. Here are some tips to help you out:
      i. Edit the file entries.html found in your userdata/csc101 folder
      ii. You can use Dreamweaver to add your entry to your page, as well as format the style of the entry.
iii. To upload your page to the web, use the “put” function in Dreamweaver. (Highlight entries.html, and click the blue up arrow)

6) I will check the following link to see if your entry exists:
   b. http://www.wfu.edu/~user/csc101
   c. Be sure to check this link to make sure your assignment appears online.
   d. If it does not appear, follow the instructions from lab to update the permissions of your website.
A new U.S. Senate bill would grant the president far-reaching emergency powers to seize control of or even shut down portions of the Internet.

The legislation announced Thursday says that companies such as broadband providers, search engines, or software firms that the government selects "shall immediately comply with any emergency measure or action developed" by the Department of Homeland Security. Anyone failing to comply would be fined.

That emergency authority would allow the federal government to "preserve those networks and assets and our country and protect our people," Joe Lieberman, the primary sponsor of the measure and the chairman of the Homeland Security committee, told reporters on Thursday. Lieberman is an independent senator from Connecticut who caucuses with the Democrats.

Because there are few limits on the president's emergency power, which can be renewed indefinitely, the densely worded 197-page bill (PDF) is likely to encounter stiff opposition.

TechAmerica, probably the largest U.S. technology lobby group, said it was concerned about "unintended consequences that would result from the legislation's regulatory approach" and "the potential for absolute power." And the Center for Democracy and Technology publicly worried that the Lieberman bill's emergency powers "include authority to shut down or limit Internet traffic on private systems."

The idea of an Internet "kill switch" that the president could flip is not new. A draft Senate proposal that CNET obtained in August allowed the White House to "declare a cybersecurity emergency," and another from Sens. Jay Rockefeller (D-W.V.) and Olympia
Snowe (R-Maine) would have explicitly given the government the power to "order the disconnection" of certain networks or Web sites.

On Thursday, both senators lauded Lieberman's bill, which is formally titled the Protecting Cyberspace as a National Asset Act, or PCNAA. Rockefeller said "I commend" the drafters of the PCNAA. Collins went further, signing up as a co-sponsor and saying at a press conference that "we cannot afford to wait for a cyber 9/11 before our government realizes the importance of protecting our cyber resources."

Under PCNAA, the federal government's power to force private companies to comply with emergency decrees would become unusually broad. Any company on a list created by Homeland Security that also "relies on" the Internet, the telephone system, or any other component of the U.S. "information infrastructure" would be subject to command by a new National Center for Cybersecurity and Communications (NCCC) that would be created inside Homeland Security.

The only obvious limitation on the NCCC's emergency power is one paragraph in the Lieberman bill that appears to have grown out of the Bush-era flap over warrantless wiretapping. That limitation says that the NCCC cannot order broadband providers or other companies to "conduct surveillance" of Americans unless it's otherwise legally authorized.

Lieberman said Thursday that enactment of his bill needed to be a top congressional priority. "For all of its 'user-friendly' allure, the Internet can also be a dangerous place with electronic pipelines that run directly into everything from our personal bank accounts to key infrastructure to government and industrial secrets," he said. "Our economic security, national security and public safety are now all at risk from new kinds of enemies--cyber-warriors, cyber-spies, cyber-terrorists and cyber-criminals."

A new cybersecurity bureaucracy

Lieberman's proposal would form a powerful and extensive new Homeland Security bureaucracy around the NCCC, including "no less" than two deputy directors, and liaison officers to the Defense Department, Justice Department, Commerce Department, and the Director of National Intelligence. (How much the NCCC director's duties would overlap with those of the existing assistant secretary for infrastructure protection is not clear.)

The NCCC also would be granted the power to monitor the "security status" of private sector Web sites, broadband providers, and other Internet components. Lieberman's legislation requires the NCCC to provide "situational awareness of the security status" of the portions of
the Internet that are inside the United States -- and also those portions in other countries that, if disrupted, could cause significant harm.

Selected private companies would be required to participate in "information sharing" with the Feds. They must "certify in writing to the director" of the NCCC whether they have "developed and implemented" federally approved security measures, which could be anything from encryption to physical security mechanisms, or programming techniques that have been "approved by the director." The NCCC director can "issue an order" in cases of noncompliance.

The prospect of a vast new cybersecurity bureaucracy with power to command the private sector worries some privacy advocates. "This is a plan for an auto-immune reaction," says Jim Harper, director of information studies at the libertarian Cato Institute. "When something goes wrong, the government will attack our infrastructure and make society weaker."

To sweeten the deal for industry groups, Lieberman has included a tantalizing offer absent from earlier drafts: immunity from civil lawsuits. If a software company's programming error costs customers billions, or a broadband provider intentionally cuts off its customers in response to a federal command, neither would be liable.

If there's an "incident related to a cyber vulnerability" after the president has declared an emergency and the affected company has followed federal standards, plaintiffs' lawyers cannot collect damages for economic harm. And if the harm is caused by an emergency order from the Feds, not only does the possibility of damages virtually disappear, but the U.S. Treasury will even pick up the private company's tab.

Another sweetener: A new White House office would be charged with forcing federal agencies to take cybersecurity more seriously, with the power to jeopardize their budgets if they fail to comply. The likely effect would be to increase government agencies' demand for security products.

Tom Gann, McAfee's vice president for government relations, stopped short of criticizing the Lieberman bill, calling it a "very important piece of legislation."

McAfee is paying attention to "a number of provisions of the bill that could use work," Gann said, and "we've certainly put some focus on the emergency provisions."

**Last updated at 9:14 p.m. PT.**
Declan McCullagh has covered the intersection of politics and technology for over a decade. E-mail Declan.