Securing America's Future:
The Cybersecurity Act of 2012

Statement of Stewart A. Baker
Partner, Steptoe & Johnson LLP
Visiting Fellow, Hoover Institution, Stanford University

Before the Homeland Security and Governmental Affairs Committee
United States Senate

February 16, 2012

Mr. Chairman, Ranking Member Collins, members of the committee, it is an honor to testify before you on such a vitally important topic. I have been concerned with cybersecurity for two decades, both in my private practice and in my public service career, as general counsel to the National Security Agency and, later, to the Robb-Silberman commission that assessed U.S. intelligence capabilities on weapons of mass destruction, and, more recently, as assistant secretary for policy at the Department of Homeland Security. In those two decades, security holes in computer networks have evolved from occasionally interesting intelligence opportunities into a full-fledged counterintelligence crisis. Today, network insecurity is not just an intelligence concern. It could easily cause the United States to lose its next serious military confrontation.

Moore's Outlaws: The Exponential Growth of the Cybersecurity Threat

Our vulnerabilities, and their consequences, are growing at an exponential rate. We've all heard of Moore's Law. What we face today, though, are Moore's outlaws: criminals and spies whose ability to penetrate networks and to cause damage is increasing exponentially thanks to the growing complexity, vulnerability, and ubiquity of insecure networks. If we don't do something, and soon, we will suffer network failures that dramatically change our lives and futures, both as individuals and as a nation.

It doesn't take a high security clearance or great technical expertise to understand this threat. It follows from two or three simple facts.

Fact One. Breaking into computer networks to steal secrets has never been easier, despite all the security measures we encounter on those networks.

Why do I say that? Simple. In recent months, we have learned that some of the most security-conscious institutions on the planet have been compromised. HBGary, RSA, Verisign, and DigiNotar are all in the network security business; they understand how to protect secrets on line -- if anyone does. But RSA was electronically attacked and its most important business secrets, the keys to its security business, were stolen. HBGary lost control of its CEO's email correspondence to a group of online vigilantes, and its CEO lost his job as a result. DigiNotar, a Dutch entity that issues online credentials, was compromised by a hacker working with Iranian security forces. Six weeks after the breach became public, DigiNotar was out of business. I

think it's fair to say that these security-conscious companies would have done whatever they could to prevent these disclosures, but they failed. They were unable to secure their networks.

Actually, the same is true for governments. The Defense Department used to say that attacks on its systems had never penetrated the classified networks. Now it has disclosed that this is no longer true. Defense contractors have also been compromised, and with them, the designs for our most recent weapons systems.

That is the first fact: No network, no matter how important its secrets and no matter how security conscious its owner, can be seen as secure in today's world. Attackers have an excellent chance of breaking in and stealing secrets. And here is the second:

Fact Two. Once the attackers are in, they don't have to stop at stealing secrets. They can cause severe physical damage just by manipulating the digital systems they have compromised.

When I was at DHS, we demonstrated that hackers could cause a large generator to self-destruct, just by sending the generator commands over the network. More recently, the Stuxnet malware is believed to have crippled Iran's uranium enrichment efforts for months, simply by infecting the computerized industrial control system responsible for Iran's centrifuges. That was good news for people who think that Iran's nuclear program is dangerous. But Stuxnet was also a proof of concept, showing that network flaws can be used to cause massive damage to any machinery that relies on computerized industrial controls.

And what machinery runs on such controls? Pretty much everything necessary to sustain our society: refineries, pipelines, electric power, water, and sewage systems. Worse, the industrial control systems that run these necessities are not really designed with cybersecurity in mind. In fact, there is reason to believe that Windows networks running on the Internet are much more secure than industrial control systems. At a minimum, we can say with confidence that industrial control systems are no better protected than the systems that failed at RSA, Verisign, HBGary, and DigiNotar.

Cyberweapons pose a real threat to the United States. Those two facts lead to a third, common-sense conclusion: Any nation that feels the need to prepare for a military confrontation with the United States has already begun developing cyberweapons. Cyberweapons are especially potent against the United States. That's because they are deniable; figuring out who has launched a cyberattack will be very difficult, making our other military assets less useful in deterring attacks. Cyberweapons are also asymmetric; they cause more harm in developed nations than in less advanced societies. And perhaps most importantly, such weapons can overturn the American war experience of the last sixty years – that conflicts will be fought far away, at a time and place of our choosing. Any nation expecting a conflict with the American military would be enthusiastic about developing a weapon that can cause massive civilian suffering on our home front before a single shot has been fired on the battle lines.

Now that such a weapon is within their reach, the impact could be unprecedented. We have no experience with losing large parts of our power, refinery, water and sewage systems all at once. The closest we've come was New Orleans after Katrina. And there, everyone knew beforehand

that the disaster was coming. Preparations had been made, and most people left the city well in advance. They went to places where the infrastructure still worked, while organized military and civilian relief efforts rapidly moved in to help those who remained. Even so, the breakdown in order and the human suffering was extreme.

Thanks to growing cyber insecurity, all Americans now live in a digital New Orleans, with Katrina just offshore. And not one Katrina, but many. Computer exploits that we once thought were the work of large nations such as Russia or China now seem to be within the capability of countries like Iran and North Korea. If I am right that computer insecurity continues to grow worse each year, then the sophistication needed to launch a cyberattack will continue to decline, and soon such attacks will be within the capability of criminal gangs and online vigilantes like Anonymous.

Disaster is not inevitable. We can head this threat off if we treat it seriously. We may have years before suffering an attack of this kind. We do not have decades. We must begin now to protect our critical infrastructure from attack. And so far, we have done little.

The Cybersecurity Act and Its Critics

The committee and the bipartisan group that has worked with the Majority Leader deserve great credit for producing a historic comprehensive legislative package to deal with this grave threat. The bill does three big things. First, it seeks to improve the cybersecurity of the infrastructure industries on which our lives and social order depend. Second, it sets aside the legal restrictions and doubts that have made it hard to share security information between government and industry. And third, it reforms the federal information security standards process.

Of these, the most important is the title dealing with critical infrastructure, and I will focus my testimony on it. This part of the bill will no doubt encounter resistance. The business community is quick to condemn anything that smacks of new government regulation. Information technology companies have achieved enormous success in recent decades and have gone largely unregulated. They want to stay that way.

They argue that information technology is too fast-moving and technically complex for government to regulate. And that's not completely wrong. It is a fool's errand to address network vulnerabilities by adopting command-and-control regulations specifying particular security measures. A new regulation takes two to three years to wend its way through notice and comment and other mandated procedures. In three years, malware will go through several generations, and attacks will evolve many times. Specifying particular security measures by regulation will not work.

But neither will *laissez-faire* reliance on the private sector. We do not expect General Motors to field its own antimissile defenses in the event of a nuclear attack. And we cannot expect private power or oil companies to stand alone against calculated attacks from the militaries of half a dozen nations. I believe that the bill, with a few modifications, charts a way to improve private sector security without resorting to command and control regulation.

Another source of resistance comes from advocates who claim that this bill is somehow similar to the Stop Online Piracy Act, or SOPA. If the bill reaches the floor, they threaten, it will meet the same fate as SOPA.

Well, to paraphrase Sen. Bentsen in the 1988 vice-presidential debate, I knew SOPA, I opposed SOPA, and Mr. Chairman, this bill is no SOPA.

I took a very early stand against SOPA, and I'm proud to have played a role in forcing its reconsideration. SOPA was a bad idea because it would have given a little help to one industry while making everyone who uses the Internet much less secure. That criticism of SOPA struck a chord with Americans because we all use the Internet with a nagging fear that our security is at risk. That security concern was at the heart of the early opposition to SOPA. This bill, in a real sense, is the opposite of SOPA. It addresses the entirely justified security concerns of ordinary users.

There is another reason not to heed the advocates who oppose this title. They're the guys who got us into this fix.

Three Presidents in a row have warned against cybersecurity risks, and three have tried to do something about it. All have been stymied by business and privacy advocates acting in alliance. A dozen years ago, President Clinton's administration proposed that the Defense Department build tools to check Internet traffic sent to DOD sites, not just for spam but for malware that might be sent by foreign governments. In response, business and privacy groups rose up, claiming that this would somehow violate the rights of people communicating with the government. The proposal was killed in Congress. Today, after what may be the most massive loss of weapons technology and other secrets in history, we are only beginning to build an Einstein system that does for civilian systems what President Clinton was not allowed to do.

We've had a lost decade in cybersecurity. The government bears some responsibility for that lost decade, but those who counsel inaction bear more. We followed their advice, and the threat is far worse now than it was ten years ago. If we follow their advice again, we will face a crisis much sooner.

Unpacking the Critical Infrastructure Protection Proposal

In fact, if I may turn to the contents of the bill, I fear that it has already been weakened unduly by those who want us to do nothing.

That is not to criticize the overall thrust of the bill. The title on critical infrastructure is in general a well-considered and coherent approach. It starts with a government assessment of the industries where the risk is greatest. See section 102. Based on the assessment, individual systems or assets deemed to be most at risk are, on an industry sector-by-sector basis, designated as "covered critical infrastructure." Section 103. Next, performance requirements to mitigate those risks are adopted for each industry. Section 104. Finally, adherence is enforced by requiring the owner of covered infrastructure to certify compliance (or to obtain a third-party assessor's certification of compliance) with the performance requirements. Section 105.

This broad structure is meant to solve the problem of how to regulate a fast moving and complex technology. It does so by leaving as much discretion as possible in the hands of the private sector. It gives the private sector preferential input into the process of assessing and identifying covered critical infrastructure. Performance requirements are supposed to be established, if at all possible, based on private sector proposals or existing industry standards. What's more, the title doesn't call for government simply to tell industry what security technologies to adopt. The point of the process is to identify the risks, warn industry of those risks, and challenge industry to develop standards and adopt measures that industry finds best adapted to the risks.

Done well, an approach of this kind is both more demanding and more flexible than traditional regulation. The government sets the bar, and it is up to industry to find the best way to get over it. That makes the approach more flexible than ordinary regulation. But if hackers find new ways to compromise critical networks, then industry measures that once were good enough must now be strengthened, automatically and without a new regulation. That makes the system more demanding than ordinary regulation. It's a good solution.

In several details, however, the bill fails to follow through on its overall approach.

How many deaths does it take before security matters? First, because the bill imposes no obligations whatsoever on systems or assets that are not designated as "covered critical infrastructure," the process of designation is a big deal. If an asset is not designated as "covered critical infrastructure," then the owner has no obligation under the bill to guard against attack by hackers, criminals, or nation states, leaving those who depend on the asset unprotected. So, the standards for prioritizing industries and designating systems or assets are crucial.

Yet the standards currently included in the bill for designating "covered critical infrastructure" are bound to leave huge swaths of important systems unprotected. The bill states that the Secretary of Homeland Security may "only designate a system or asset as covered critical infrastructure if damage or unauthorized access to that system or asset could reasonably result in . . . (i) the interruption of life-sustaining services, including energy, water, transportation, emergency services, or food, sufficient to cause (I) a mass casualty event that includes an extraordinary number of fatalities; or (II) mass evacuations with a prolonged absence; (ii) catastrophic economic damage to the United States . . . or (iii) severe degradation of national security of national security capabilities, including intelligence and defense functions. "

Let's unpack that first test. It says that a system or asset cannot be regulated under this bill unless a cyberattack on it would so interrupt life-sustaining services that it would cause "a mass casualty event that includes an extraordinary number of fatalities." Really? So an individual infrastructure owner, such as a rural electricity provider, has no responsibility under this title if it can show that an undefended cyberattack would only cause an *ordinary* number of fatalities?

How many dead Americans is that, exactly? Under the bill as written, any business that wants to avoid being regulated can take the government to court and argue that it is exempt from obligation under the law because only a few its customers will actually die if its security fails. That's wrong. The courts are going to have to give effect to every adjective in this bill, from

"extraordinary" numbers of fatalities, to "catastrophic" economic damage and "severe" degradation of national security. Do we really want to see companies escape any security obligations by arguing that their failures will of course degrade national security or cause economic damage, but not severe degradation or catastrophic damage? This would be a better bill if those adjectives were reconsidered.

The information technology exclusions. My second concern is that the bill gives the IT industry too much of a free pass. The bill expressly prohibits the inclusion of any "commercial information technology product, including hardware and software" within the category of "covered critical infrastructure."

This is odd. Commercial information technology products are certainly part of the problem. Why shouldn't they be part of the solution?

Of course IT companies have legitimate concerns about how regulation would affect their ability to innovate, especially on a global basis. Perhaps it doesn't make sense to treat individual platforms, such as Windows, as covered infrastructure sectors. But at the same time, we cannot ask the owners of covered networks to improve security without help from their IT providers.

The bill as drafted probably does allow the government to set standards for IT companies indirectly. (Thus, the government could endorse a performance standard like this one: "Operating systems utilized by covered critical infrastructure must enable authentication of each machine on the network by means of a trusted processing module or equivalent hardware-based technique.") Assuming this is consistent with the statute, the exclusion of commercial IT products from covered infrastructure may be tolerable.

But such an indirect approach is put at risk by a second set of limits written into the bill. These exclusions would prevent the government, when establishing performance requirements, from requiring the use or regulating the design of commercial information technology products and related services. This language is much too broad. It would cast doubt on any performance standard that applies by its terms to commercial hardware or software used by critical industries, including the example that I gave above.

It seems to me that, if IT products are not to be treated as a covered infrastructure, the companies that make them should be encouraged to provide very specific forms of security support to those of their customers who are covered. Put another way, the IT industry can reasonably ask for one of these exclusions, but not both.

Immunity for operators who have no statutory obligations. By the same token, the bill imposes obligations on the owners of critical infrastructure but not on the operators of critical infrastructure. This seems to exclude anyone who acts as an outsourced provider to the actual owner. So if a telecommunications company outsources its hardware operation to a foreign switch manufacturer or a pipeline company hires an IT company to run its networks, the obligations of the bill do not apply to the switch manufacturer or the IT company. This is less troubling, I suppose, than the blanket exclusion of all commercial IT products, since obligations

imposed on the owner may be passed on to the operator. But if the operator isn't subject to regulation, why should we reward the operator as well as the owner with an immunity from punitive damages?

Cutting through the regulatory drag in an emergency. Finally, my biggest concern about the bill has to do with the risk of regulatory atherosclerosis. The process set forth in the bill is very friendly to industry, deferring at every turn to industry-led standards and solutions. In general, this is a good idea. But the end result is a process that will take many years to implement, especially in sectors that decide to resist rather than comply with the intent of Congress.

Here's my quick assessment of the likely elapsed time from enactment to actual implementation of security measures by a reluctant industry.

- **Risk assessments.** The top-level risk assessment must be done in 90 days, but there is no deadline for doing sectoral risk assessments. Those could take at least a year and probably two to finish, and they must be completed before the remaining steps can be taken.
- **Designation.** The government must explain its criteria for designation, and it appears that it must individually identify the companies to be designated. What's more, every decision it makes can be challenged in court, which will make the government cautious and slow in making designations. This step too will take at least a year or two in many sectors. And that's not the end. The bill chooses the slowest possible judicial review process, sending appeals first to district court and then up on appeal. Any industry that appeals its status could buy two or three more years before the next step can be taken.
- **Set performance requirements.** The bill's preferred method for setting performance requirements is to rely on stakeholder proposals or existing industry standards. But if, after all of these proposals are submitted and reviewed, they are insufficient to address the security threat at issue, then and only then can the Secretary of Homeland Security, still in consultation with industry, develop satisfactory requirements. That process too could easily take another two years.
- **Enforce the requirements.** Once all of that is done, and an enforcement regulation has been written, each covered company must certify that it has adopted measures that it considers sufficient to meet the applicable performance requirement. (Alternatively, the company can choose to wait for the government to go through the long process of creating, training and testing up an entire new class of third-party assessors.) If the government suspects that the company's certification is false, it can conduct its own assessment, but it's not completely clear that it can impose any new requirements; it may be that the company can wait to be sued for a false certification and then avoid any penalty by adopting a new set of security measures and claiming that it has remediated any failure in a timely way. That could be very lengthy and messy, but let's figure a year for the certification and another year to sue a recalcitrant company.

Based on those calculations, a company that simply exercises rights conferred by the title could delay any cybersecurity measures for eight to ten years after enactment. That's another lost decade.

I don't mean to suggest that the risk of delay should be solved by getting rid of these lengthy processes. They are necessary to get the benefit of the private sector's creativity and flexibility in dealing with security problems. They should be retained in most circumstances.

But clearly there are some problems that we cannot wait a decade to solve. In an emergency, the government must have authority to skip or compress any of the procedures described above. If a security threat to a particular company or sector plainly threatens the lives of Americans, the department should be free to demand prompt action by the company. The company may remain free to choose the solution, but the government must be able to insist that the solution work and that it be implemented as promptly as necessary to save lives. That, after all, is the purpose of this bill. Without authority to waive time-consuming procedures in an emergency, the bill will fail in that purpose. I know such authorities are hard to draft, so I've attached one possible version to my testimony.

Conclusion: Our Best Hope to Avoid a Predictable Disaster

In closing, let me return to my main theme. We face a crisis. Cybersecurity is bad and getting worse. Civilian lives, and our ability to win the next war, depend on solving our security problems. We have to do that without losing the great benefits that a largely unregulated global IT industry had brought to us. But we cannot let advocates for the status quo condemn us to another lost decade of growing insecurity. This bill, even with its flaws, is our best hope to head off a perfectly predictable disaster.

We are all living in a digital New Orleans. No one really wants to spend money reinforcing the levees. But the alternative is worse.

And it is bearing down on us at speed.

Possible Amendment to Deal with Imminent Threats

Stewart Baker

SEC XXX. RESPONDING TO IMMINENT THREATS

(a) Notwithstanding the other sections of this Title, in the event that the imminence or existence of a cybersecurity emergency as defined in section (b) makes it impracticable to complete one or more of the steps below in accordance the procedures established under this title the Secretary shall have the authority to promptly —

(1) identify cyber risks that have created the cybersecurity emergency within one or more affected sectors;

(2) designate the covered critical infrastructure and any systems or assets that must respond to these risks;

(3) develop risk-based cybersecurity performance requirements that address the identified cyber risks;

(4) require, within a period of time determined by the Secretary, that each owner of covered critical infrastructure, whether identified under this section or section 103 of this title, implement security measures sufficient to satisfy the risk-based security performance requirements established under this section and promptly —

(A) certify in writing to the Secretary that the owner has developed and effectively implemented security measures sufficient to satisfy the risk-based security performance requirements established under this section; or

(B) submit a third-party assessment in accordance with Section 104(d);

(5) enforce any requirement of this section; and

(6) expedite the implementation of any other provision of this title.

(b) The Secretary shall declare that a cybersecurity emergency exists only when a cybersecurity risk to a particular critical infrastructure sector --

(1) cannot be prevented in timely fashion by adhering to the procedures set forth in sections 102 through 107 of this title; and

(2) poses a present or imminent threat of

(A)the interruption of life-sustaining services, including energy, water, transportation, emergency services, or food, sufficient to cause—

(i) a mass casualty event that includes an extraordinary number of fatalities; or

(ii) mass evacuations with a prolonged absence;

(B) catastrophic economic damage to the United States including—

(i) failure or substantial disruption of a United States financial market;

(ii) incapacitation or sustained disruption of a transportation system; or

(iii)other systemic, long-term damage to the United States economy; or

(C) severe degradation of national security or national security capabilities, including intelligence and defense functions.

(c) Judicial review in accordance with section 103 shall be available as provided in that section, but no stay shall be granted of any order, determination, directive or other action under this section unless the party requesting the stay posts a bond fully sufficient to cure any harm that may be caused by failure to implement the stayed order, determination, directive, or other action.