STATEMENT

OF

STEWART A. BAKER
PARTNER
STEPTOE & JOHNSON LLP

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

HEARING ENTITLED

"CYBER SECURITY: DEVELOPING A NATIONAL STRATEGY"

PRESENTED ON

APRIL 28, 2009

Chairman Lieberman, Ranking Member Collins, and members of the Committee, I want to begin by thanking the Committee for holding this timely hearing. As a nation, we have never depended more on information technology (IT) networks. Standardized IT networking is often credited with a productivity renaissance, and it has changed the everyday lives of Americans in profound ways. In fifteen years, decentralized networks have moved from novelty uses like monitoring communal coffee machines to managing financial assets, telecommunications, and the electric grid.

That's both good news and bad, because this revolutionary new technology poses real risks. We trust far more of our critical assets to IT networks than we once did, and security vulnerabilities that may have been tolerable fifteen years ago can have devastating consequences today.

Let me give you just one example of the new risks that all this connectivity has introduced into our lives. It's the story of a man named Howard Crank; I heard it from his stepdaughter. Earlier this year, in January, Howard Crank was living quietly at home when he learned that he had won a prize in a Spanish lottery. He needed the money. He was 73 years old, a retired Air Force veteran living on a pension in a modest California duplex. Diabetes had forced the amputation above the knee of both his legs. His wife's health was not good. But he could afford a computer, and it opened new worlds to him. Even a housebound vet could travel the world on the Internet.

The Internet, it appears, is how he discovered that he'd won the lottery. Of course, it turned out that there were transfer taxes to pay before the winnings could be sent to him. It was expensive, but his share of the lottery was also growing – at one point his winnings reached $115 million.

Howard Crank started sending money to clear the taxes and release the funds. His life savings were $90 thousand. He sent that.

It wasn't enough, so he took out a loan secured by his home and sent that. A few weeks later, he took out a second loan on the house and sent that. He maxed out two credit cards and sent that. Perhaps $300 thousand went to Spain. Still not enough. He asked his stepdaughter for $40 thousand.

She thought that was odd. And when he was hospitalized a few weeks later with a broken femur in what remained of his left leg, she checked his financial records. She found that Howard Crank had ruined himself and his wife in response to an apparent Internet hustle. The Spanish scam artists disappeared without a trace. Crank died of a heart attack before he could provide details.

"I think he probably knew it was a fraud at the end. But he was hoping against hope. He'd sent them so much money already, and they were so convincing," his stepdaughter says. "By the end he'd lost his zest for life. He was desperate."

His 79-year-old widow will lose her home and is likely to be forced into bankruptcy by the remaining debts.

Now I don't tell that story because Howard Crank was the victim of some clever security breach. I tell it because the source of the problem was how close the fraudsters could get to him. He would never have let a con man into the quiet life he and his wife were living. But the Internet brought con men from all over the world to his duplex. Just as it bring thieves and spies and soldiers from all over the world to our banks and government offices.

And for one reason more. Howard Crank got real pleasure and value from using the Internet. He could find previously obscure nuggets of information, perhaps the whereabouts of old Vietnam War friends he'd lost touch with, or new charities he could to add to the three dozen he already supported. But in the end, all that connectivity took far more from him, all at once, than it had given in years earlier. So too for us. We may be too cynical to fall for a Spanish lottery email. But more sophisticated attackers will find better ways to get close to us, to know our families, and our finances, and our weaknesses. And if we don't find a way to shore up our defenses and above all to bring accountability to the Internet, more and more Americans will lose everything to organized crime.

And crime is just the most obvious risk. When nation states bring their resources to bear on the exploitation of network vulnerabilities, the danger is even greater. When I was General Counsel of the National Security Agency in the early 1990s, network attacks were rare and difficult. When I came to the Department of Homeland Security in 2005, network attacks were

commonplace and highly successful. It's as though the typical score in a soccer game had gone from 1-0 in the 1990s to something like 247-189 today.

The CSIS Commission on Cybersecurity for the 44th Presidency deserves great credit for thoughtfully addressing the crisis that we face. I participated in some of the Commission's proceedings, and I join in many of the recommendations that Commission made. But not all of them. Today, I would like to address two topics, one where I disagree with the Commission and one where I tend to agree. The first, where I disagree, concerns organization. The second, where I agree, touches on the relationship between the federal government and the private sector.

I. The principal organizational recommendation made by the Commission concerns the role of the White House. The Commission recommends that responsibility for cybersecurity be lodged with a new Assistant to the President. This assistant would be supported in the first instance by a National Security Council directorate. As further support, the Commission recommends creating a National Office for Cyberspace, or NOC, in the Executive Office of the President. This office would absorb some of the cybersecurity responsibilities now assigned to DHS, most notably the National Cyber Security Center, or NCSC. Below these offices, DHS and other agencies would continue to exercise their existing authorities, but with new vigor and coordination arising from the clout of the Assistant to the President, the NSC, and the new NOC.

Without intending it, I've become something of an expert in the process of creating new government organizations, having worked to establish two of the three most recent Cabinet departments. I helped Shirley Hustedler start the Education Department in the late 1970s, and at DHS, I started the DHS Office of Policy. That was a startup within a startup. The more I've seen of government reorganizations, the more skeptical I've become about their value, and I'm especially skeptical about the recommendation to create a NOC.

Let me explain why. There is a kind of lifecycle to proposals for new governmental organizations. In the first stage, proposals for organizational change begin to gain momentum -- almost always because the existing organization of government is flawed. After all, no one suggests changes when things are going well. Sometimes there's been a shocking failure, such as the 9/11 attacks that led to the creation of DHS. Sometimes the flaw is a lack of governmental focus on a mission that seems more important than before, as with the Education Department. But we always begin with an existing organization whose flaws have suddenly become especially prominent.

The second stage, when proposals for organizational change become concrete, requires an exercise of imagination. The new organization has to be envisioned. Since the whole point of the new organization is to cure the failings of the old organization, I think it's fair to say that the proponents of change never imagine an understaffed, overworked agency that drops balls. No. More or less by definition, an organization that does not exist does not have any flaws. So there's a great temptation to give this new organization great responsibility. After all, the old agencies have sometimes failed, and the new agency has not.

Unfortunately, that's only the second stage. In the third stage, the new organization actually begins work. In the glare of publicity it takes up its new responsibilities. But as a brand-new agency, it has to hire staff, find space, let contracts, arrange for IT support, and lease copiers, all before it can begin to carry out the missions that it has been assigned. Meanwhile, the agencies that lost ground in the reorganization snipe from the sidelines or make a bid to recapture their old turf. Six months after it's been created, the new agency is still struggling to put in place the basic capabilities that any agency needs to function. Instead of the ideal organization imagined by lawmakers and commission members, the new agency is all too

flawed. Only after years of effort does the reorganization begin to produce improvements that the outside world can see.

I've lived that cycle. I've helped write reports that called for the creation of new organizations to respond to existing agencies' flaws. I've joined new organizations full of enthusiasm for the newly imagined perfection that they will embody. And I've labored to deliver perfection in offices that had no light bulbs, no staff, and no way to move paper around the office.

It's that experience that makes me dubious about creating a National Office for Cyberspace. I know that some in Congress find that proposal appealing. The Cybersecurity Act of 2009, recently introduced in the Senate, would create a new office within the Executive Office of the President (EOP) to manage cybersecurity. I also understand the Commission's frustration with DHS. Many of its members dealt with DHS's cybersecurity organization when it was deep in Stage Three of the cycle I have described. In discussing why cybersecurity should be managed from the White House rather than DHS, the Commission says as much. "Managing a complex international effort involving several large and powerful departments would be difficult for any agency, much less one that is still in the process of organizing itself. Although, [DHS's] performance has improved in recent years, our view is that any improvement to the nation's cybersecurity must go outside of DHS to be effective."

Here, I believe that the commission, and others who wish to strip DHS of cybersecurity responsibilities, fall prey to the perfection of imagined alternatives. But the problems that DHS has faced in organizing itself are likely to be repeated in any new agency created as a substitute for DHS. If the commission is concerned about the difficulty of an agency's improving

cybersecurity while also organizing itself, then it should be a bit more cautious about handing that task over to an agency that has not even begun to organize itself.

Compared to the perfection of an imaginary NOC, of course, DHS's flaws look serious. But the NOC will have flaws too. It will have to begin by doing what every new agency has to do – hire staff, build processes, find furniture, and let contracts while at the same time trying to carry out a mission that everyone agrees is urgent. DHS has spent the past year doing exactly that, both for the NCSC and for the Einstein deployments and other operational tasks assigned to it by the last Administration. If DHS has only begun to build that capability after a year, what makes us think that the NOC can organize itself more quickly?

The best argument for putting a large office with quasi-operational responsibilities in the Executive Office of the President is to give it clout, or at least visibility. But clout is a matter of Presidential will, not boxology. The Office of National Drug Control Policy has been in the Executive Office of the President since 1988, but it's fair to say that its clout has varied substantially over the years. By the same token, no one thinks that the Defense or Justice Departments need to be in the White House to demonstrate how seriously every President takes them.

And the price o f that imagined clout is high. For the President, of course, putting the NOC in the Executive Office of the President means that responsibility for its success or failure will fall squarely on his shoulders. If the new office turns out as well as we imagine, that may work out fine. But if not, it is the President's managerial decisions that will be criticized. What's more, finding staff and funding and space for a new White House office will be a challenge. Finally, the battle rhythm of any part of the Executive Office of the President leaves little room for long-term work like drafting regulations, setting standards, or overseeing

cybersecurity centers. Inevitably, staff will be pulled into the urgent crises that arise every day at the top of their organization. Important projects that can be postponed in the face of emergencies will be postponed, again and again.

In short, I urge the committee, and the Administration, to be cautious about pinning its hopes to a NOC that has no flaws because it doesn't exist. If we start over again, we're likely to be disappointed again. DHS's execution of its responsibilities has certainly not been perfect, but it has spent much of the last year improving on its record. It has able new leadership and a head start on creating the capabilities it needs. I would be inclined to build on that foundation rather than starting over.

For the same reasons, I would be cautious about restructuring all of the advisory committees and information sharing arrangements that DHS administers. First, although I share many of the frustrations that the Commission expressed with the current structure, I question whether the structure of federal advisory committees will make much difference in our long-term preparedness for network attacks. Many of the problems identified by the Commission – a proliferation of Washington representatives and a decline in CEO participation, for example – can be solved without throwing out the current structure. If the President meets regularly with the NSTAC and makes it clear that he expects to be meeting with CEOs, then CEOs will soon fill the NSTAC's ranks, no matter where it is housed.

II. Now let me turn to the relationship between government and the private sector on network security. There is no doubt that it needs to evolve further. The Commission is correct when it says that industry will need help and guidance, perhaps even regulation, to meet this threat. Left to its own devices, the private sector will only invest in network security until marginal costs equal marginal benefits. Put another way, no rational company will spend a

dollar on network security to prevent ninety-nine cents worth of loss. Private sector security is inevitably focused on quantifiable, predictable losses, such as theft of services. But not every intruder is a thief or a fraudster. Some of them are spies and saboteurs planning a new form of warfare. Protecting civilians from warfare is not usually a task we leave to the private sector.

Recognizing the need for a government role is the easy part. What's more difficult is developing the expertise that's needed to guide the private sector. Generally speaking, the federal agencies on the civilian side of government are not as sophisticated about network defense as many private sector industries, such as banking. There is reason to believe that improvements in federal capability are likely. DHS is going to increase its own expertise substantially as it oversees the upgrading of federal civilian cybersecurity. That's an essential step if the government is to provide useful guidance to the private sector.

Even more difficult is the task of knowing how to guide the private sector. I do not want to pretend that I have all the answers here. But I think some points are plain. First, this is not an area where laws or even regulations can move as quickly as the threat. A few years ago, it was possible to imagine that improved operating system security would solve most of the problems we faced. If we had written rules then, they would have focused heavily on patches, and updates, and the responsibilities of operating system producers. But Microsoft in particular has devoted enormous resources to building security into its operating system – to making sure that programs cannot run without the user's permission.

And the result is not better security, just better malware. Hackers now often seek out flaws in applications or websites, or they try to fool users into granting permission by clicking on a file that purports to be something it is not. If we find ways to close off this avenue of attack, I fear that new avenues will be opened, and new countermeasures will be necessary. Thus, a

system in which the government imposes rigid standards on the private sector through the regulatory process seems doomed to lag behind the threats it seeks to thwart. I would urge great caution before we launch legislative and regulatory efforts to prescribe particular security measures.

Some regulatory regimes try to deal with this problem by imposing procedural rather than substantive requirements on companies -- that is, they require companies to develop and implement their own standards rather than imposing static, one-size-fits-all standards through the regulatory process. For example, the Gramm Leach Bliley Act (GBL Act) seeks to safeguard personal information held by financial institutions by requiring each institution to develop and implement its own security plan. The GLB Act sets out broad objectives for these security plans rather than requiring individual plans to contain certain specific elements. The Federal Energy Regulatory Commission (FERC) appears to be taking a similar approach with respect to cybersecurity. FERC has recently approved critical infrastructure protection (CIP) reliability standards to protect the nation's bulk power system against potential disruptions from cybersecurity breaches. These standards require owners and operators of the bulk power system to establish policies and procedures to safeguard physical and electronic access to control systems and to be prepared to recover from a cyber incident. These standards identify the assets that need to be protected and broadly outline the measures necessary to protect them. The standards, however, impose very few specific security requirements.

This approach has the advantage of flexibility. Assessing a company's current security status and being ready to respond to threats are not requirements that will go out of style. But such procedural approaches run the risk of becoming meaningless. While it might well be useful to apply these flexible standards more broadly, the government is likely to have to find a way to

provide guidance, and quite possibly binding guidance, in a way that is far speedier than our current clotted regulatory process allows.

In short, it is clear that the federal government will need to exercise more authority over the private sector to improve network security. But the usual tools – such legislation, regulation, and standards – are not sufficiently flexible or fast-moving to address the problem. Without pretending to have a complete alternative in hand, I think that the most appealing approach will combine procedural requirements, as in Gramm-Leach-Bliley, with fast-moving situationally-driven guidance from a DHS that has, and can draw on, the best security thinking in the federal government.

I thank the Committee for the opportunity to share my thoughts on this topic, and I look forward to working with you and the Department.