Statement of James A. Baker
Before the
Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security
United States House of Representatives
Regarding
"Cyber Security: Protecting America's New Frontier"

November 15, 2011

Chairman Sensenbrenner, Vice-Chairman Gohmert, Ranking Member Scott, and Members of the Subcommittee: is it an honor to appear before you to discuss the cyber security challenges facing us today. As we all know, this is a very important topic and I believe that this hearing can help us make progress on improving our cyber security posture. I would like to note at the outset that I am appearing today at the request of the Subcommittee in my individual capacity and not on behalf of any current or former employer or clients. The Department of Justice reviewed this statement and does not object to its publication. I would like to focus my remarks on a few key points today.

First, as you know the United States faces a significant cyber threat today. Many others have made that point as well so I will not belabor it. The threat comes from many sources, including nation-states and non-state actors, such as organized crime groups, terrorist organizations, and lone individuals. The money in our banks, our intellectual property, and our critical infrastructure are threatened. There is a very real risk that in a time of crisis, some parts of our critical infrastructure – electrical, water, financial, transportation, telecommunications – will not function as designed (or at all). Moreover, the means that malicious actors use to gain access to computers and computer networks to enable them to steal money and data also may enable them to take complete control of a computer or a network. Such root access may allow them to burrow into that network so that it becomes exceedingly difficult to find them and to prevent them from re-accessing the network in the future at will. Malicious actors often seek to establish such a persistent presence in compromised networks.

Presently, the United States is not fully prepared to deal with the cyber threat that we face. In other words, our defensive capabilities are insufficient to address the malicious activities that are directed against the United States. This includes federal, state, and local governments; civilian and military authorities; and the private sector. At the present time, we cannot stop the theft of funds, intellectual property, or personally identifiable information, and we cannot ensure that malicious actors will not be able to degrade or destroy elements of our critical infrastructure at a time and in a manner of their own choosing.

Although many people in government and the private sector are working overtime to find more effective ways to address these vulnerabilities, right now we cannot guarantee our cyber security. That does not mean we should just give up, but it does mean that we need to make sure we are thinking about mitigating risks that we cannot

eliminate. And we need to figure out how to improve our cyber security, protect our data and networks, and continue to carry out essential functions in a compromised and probably degraded operating environment. Put differently, we need to presume that the intruders are already inside the gates and are among us. We may not be able to detect them in every instance, so we should assume that they are already here and act accordingly.

There are many reasons why we are not prepared to fully address the cyber threat. These include technological, organizational, policy, and legal issues. Let me say a few words about each of these factors.

First, there is much we can and should do from a technological perspective to improve our cyber security. We can properly configure and update network hardware and software; we can install strong firewalls and other perimeter-based security platforms; and we can implement robust access controls and monitoring systems. In some fundamental respects, however, today's communications and information technology infrastructure is inherently vulnerable. As a result, offensive cyber activities will always have an advantage over defensive ones. Let me give three examples – the zero day threat, the supply chain threat, and the insider threat.

The zero day threat is that malicious actors will develop and distribute damaging new malware that our defensive systems cannot detect and prevent from entering our networks. To be clear, "malware" is malicious software. Many of our cyber security technologies today are focused on scanning streams of communications or computer data to look for known malware "signatures" or code. The problem is that such technology detects malware signatures that someone has seen before. Our devices look for what they are programmed to look for, which are threats that we already know about. But new malware signatures are developed and unleashed all the time and it is hard to detect something that you have not seen before. Certain tools that look for anomalous behavior on networks show promise and may improve our security profile, but again they looking for patterns of behavior that have been seen before or that they are otherwise programmed to look for based on some predictive model. They will have a hard time detecting threatening behaviors that are truly novel. This is one example of why offense has an advantage over defense in cyber security.

The supply chain problem is that it is exceedingly difficult to ensure that software, hardware, and firmware that we purchase does not contain malware or other vulnerabilities – either by design or by mistake. Technology is complex and changes frequently, and it may be hard to detect built-in vulnerabilities. The insider threat is also easy to explain and difficult to address. Either intentionally or by mistake, individuals who have access to computers, networks, and data can introduce malware into systems, fail to properly configure networks using established protocols, or purloin data and intellectual property. There are ways to mitigate such risks, but not perfectly. Those are some of the technological problems we face.

Now let me discuss briefly some of the organizational and policy problems we must confront. The federal government is not yet where it needs to be organizationally to fully address the cyber threat. The roles and responsibilities of the major governmental actors – such as the Department of Homeland Security (DHS), the Department of Defense (including the National Security Agency (NSA) and U.S. Cyber Command), and the FBI – are not yet defined thoroughly relative to each other in the cyber arena. There has been much progress in this sphere, but the government is not yet where it needs to be. As a result, too much time is spent on figuring out agency roles and responsibilities on an ad hoc basis in response to a cyber incident; information about an incident is not collected or shared as robustly as it could be shared; and the full complement of investigative and analytical resources of the government are not always as fully or as promptly used as they could be used.

Moreover, it is not yet clear what role we expect the private sector to play in protecting the United States from cyber threats. This is crucial as most of the cyber infrastructure is owned and developed by the private sector. As a result, information that the private sector possesses about cyber incidents is not shared as promptly or extensively as it could be shared with pertinent actors, and the full range of private sector defensive capabilities is not utilized or coordinated fully among private sector entities or with federal authorities.

Related closely to these organizational issues are some significant policy decisions that the United States needs to make. Not only do we have to resolve questions about which actors should be involved in cyber security, we need to decide what we want them to do in providing that security. That is the biggest policy question we face as a society – What do we want to do to protect our cyber security? For example, we have not decided what role we want the government to play in monitoring private networks; what we hope to achieve as a result of such monitoring; and how we conduct such monitoring and simultaneously protect privacy, foster innovation, and promote competition. In addition to monitoring, we also have not figured out what we want military authorities – including U.S. Cyber Command – to do to protect us. The government has built that entity, but has not yet figured out how it wants to use it. For example, should the military monitor private networks in real-time and strike back at malicious cyber actors in some fashion? How accurately should the military be able to predict the collateral effects of an offensive cyber action before it strikes? And if the military does strike back, what impact will that have on the legitimate equities of law enforcement and intelligence agencies, and who is supposed to deconflict all of that? Once decision-makers and technical experts figure out what they want to do, the military and civilian lawyers can assess the legality of those actions.

Next let me turn next to the question of the extent to which the law impedes our ability to protect cyber security. In my view, the problems that we face right now in terms of our preparedness to deal with the cyber threat are not primarily legal in nature. As I have discussed, they are mainly technological, organizational and policy-based. To be sure, there are tough legal issues that we need to confront. For example, there is a complex, intertwined set of federal and state statutes that governs this area, and many of

them contain criminal prohibitions. Proper analysis of these laws is time consuming, and in many respects the law is not clear. As a result, it can be unnecessarily risky for governmental and private entities to take certain actions to thwart cyber threats. The basic idea here is that when someone in the government or a private company asks, "Can we do this?" it can be very difficult to figure out the correct answer quickly under today's statutory framework.

There are ways to remedy this, however, and the Administration's current cyber proposal does just that when it comes to simplifying the law with respect to allowing private entities to share more easily cyber security information with the government on a voluntary basis. The proposal also includes appropriate privacy safeguards. That proposal is not a panacea, and some have criticized it from a variety of perspectives, but my point is that the statutory issues can be addressed once we decide what we want to do.

Of course, we must also address constitutional issues. There is a good case to be made that reasonable governmental activities directed at enhancing cyber security would pass constitutional muster. I do not have time here today to address fully all of the constitutional issues, but the basic point is that the Supreme Court's special needs doctrine likely would apply in the cyber security context and should provide the government with the flexibility it needs to address the threat so long as its programs are reasonably designed in light of the threat and the level of intrusion into constitutionally protected spheres.

Again, I think that what we need to be focused on right now is deciding what we as a country want to do to respond to the complex and dangerous cyber threat that we face. Lawyers obviously must be involved in that discussion. But we should not conflate tough policy choices with real or imagined legal problems.

Finally, I would like to address some of the Administration's proposals to amend the Computer Fraud and Abuse Act (CFAA) and related provisions. As the Subcommittee is well aware, criminal statutes are only one means that we must use to deter cyber criminals. Standing alone, these provisions will not address fully all of our cyber security requirements. They are an important, however, and likely will assist law enforcement agencies and prosecutors in better ensuring that cyber crime is deterred effectively and punished appropriately. In my view, these proposals will update, simplify, and strengthen the CFAA.

For example, it will strengthen the CFAA to add a provision to prohibit activities that involve knowingly causing or attempting "to cause damage to a critical infrastructure computer, and such damage results in (or, in the case of an attempted offense, would, if completed have resulted in) the substantial impairment – (A) of the operation of [a] critical infrastructure computer; or (B) of the critical infrastructure associated with such computer." In light of the severity of such a crime, the three-year mandatory minimum sentence that the Administration has proposed seems appropriate. I understand that some Members have concerns about mandatory minimum sentences in general, but I believe that such a provision is justified here to ensure that courts will sentence those

convicted of such offenses in line with the severity of the crime. In any event, I urge Congress to work with the Administration to find a set of mutually acceptable provisions to modify the CFAA and related laws that you can enact quickly.

What Congress should not do, however, is to take steps that would weaken, rather than strengthen, the CFAA. I am concerned that some proposals to modify the terms of the existing Act – in particular, those directed at modifying the scope of the term "exceeds authorized access" – would have the unintentional effect of undermining the CFAA in important respects. I understand the concerns that some have raised that the scope of the Act may be ambiguous and that government overreaching could result in individuals being prosecuted for what essentially are innocent or harmless violations of the terms of service of particular websites or services. Notwithstanding one frequently cited example (the prosecution of Lori Drew), I do not believe that the case has been made that federal prosecutors have misused the CFAA. And to the extent that Congress is concerned that such abuses might occur, it strikes me that it may make more sense to use your oversight powers to ensure that enforcement of the CFAA is properly focused on the worst offenders. Indeed, rather than amending the definition of "exceeds authorized access" under the statute, Congress could legislate a reporting requirement to ensure that you are made aware promptly of any prosecutions brought against individuals or entities for exclusively violating the terms of service of a website.

Unnecessarily restricting the scope of the CFAA on the basis of one or two cases will needlessly tie the hands of prosecutors to the advantage of those who use computers to undertake fraudulent activities and abuse their otherwise authorized access to computers to harm others. Do we really want to make it harder for the government to prosecute individuals who abuse their authorized access to immense databases at financial institutions, social networking sites, and email providers to steal money or sensitive personal information? Do we want to give the government fewer tools to combat identity theft and fraud using computers? Bad facts in one case should not make bad law.

In closing, I recommend that the Subcommittee move quickly to enact some version of the Administration's proposal. As the Administration has acknowledged, the current proposal will not address fully all of the cyber security challenges that we face today. But the proposal is a good start that will have to be followed up by further legislative and executive branch action in the future. This is not a problem that is amenable to simple solutions, but we need to start moving in the right direction as quickly as possible. Our adversaries are not waiting for us to act.