COMPUTER & COMMUNICATIONS
INDUSTRY ASSOCIATION
Open Markets, Open Systems, Open Networks

October 12, 2007

The Honorable John Dingell
Chairman
House Committee on Energy and Commerce

The Honorable Edward Markey
Chairman
Subcommittee on Telecommunications and the Internet

The Honorable Bart Stupak
Chairman
Subcommittee on Oversight and Investigations

Dear Chairman Dingell, Chairman Markey and Chairman Stupak:

On behalf of the Computer & Communications Industry Association I thank you for your letter of October 2. Among other things, you asked for our views regarding the potential for privacy breaches in the face of the Protect America Act of 2007 (Public Law 100-55.) You asked whether the rising number of government databases increases the likelihood of data breaches, and whether or not government might use data for purposes other than those for which they were intended.

We think it is safe to answer "yes" in each case. All other things being equal, more databases will yield more data spills since a database that does not exist cannot be compromised in the first place. Similarly, if misuse follows opportunity – and computer crimes and misuse most certainly do – more incidents of misuse of data are sure to come.

You are right to seek tight controls on government data dissemination. You should, in our view, demand increased efforts in maintaining the integrity of those data against intruders as well as government personnel who may lack authorization to access it.

We cannot say with any certainty what law enforcement officials, the national security community or any other sector of government may do with the information they obtain. Recent experience suggests that we live in increasingly insecure times, both in terms of attackers' sophistication and the ability of most major agencies to manage the technology that they have. Indeed, the Computer Security Institute, among others, has tracked this issue for years and come to the conclusion that the problem is not improving.

Your letter cites annual FISMA reports that give concise snapshots of government security practices. These reports serve a useful purpose in evaluating the broad landscape of computer security in government, but do not appear especially useful in determining whether specific, highly sensitive data are in fact secure.

We reach this conclusion because the Government Accountability Office has for each of the past 10 years designated information security a "High-Risk Issue," and this despite dozens of reports calling for changes in how the government handles sensitive data.

Federal information security is still a high-risk proposition because of the government's failure to do what it must to secure its networks from risks both inside and out.

The GAO has issued many reports, but one recently presented to the Committee on Oversight and Government Reform may sum up today's regrettable federal landscape best.

The June 7, 2007 report "Agencies Report Progress, but Sensitive Data Remain at Risk" (GAO-07-935T) is unsparing in its criticism of government data security practices. It underscores the importance of "watching the watchmen." Gregory Wilshusen, GAO Director of Information Security Issues writes:

> Recently reported information security incidents at federal agencies have placed sensitive data at risk. For example, personally identifiable information about millions of Americans has been lost, stolen, or improperly disclosed, thereby exposing those individuals to loss of privacy, identity theft, and financial crimes. The wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches underscores the need for improved security practices.
>
> As illustrated by these security incidents, significant weaknesses in information security controls threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of federal agencies. Almost all of the 24 major federal agencies had weaknesses in information security controls. Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information.

This critique is revealing, to be sure, but does not address individual agencies. Nonetheless, it points to eight separate incidents that have appeared in national headlines since April 2006. The vast majority of agencies were deficient in each of five key security areas.

The GAO examined FBI information security in its report "FBI Needs to Address Weaknesses in Critical Network" (GAO 07-68.) Auditors were no more sparing in their assessment of the agency than they had been of the government as a whole. As the Office said on April 30, 2007:

> Certain information security controls over the critical internal network were ineffective in protecting the confidentiality, integrity, and availability of law enforcement and investigative information … Taken collectively, these weaknesses place sensitive information transmitted on the network at increased risk of unauthorized disclosure or modification, and could result in a disruption of service.
>
> These weaknesses existed, in part, because FBI had not fully implemented key information security program activities for the network reviewed … In commenting on a draft of this report, the FBI Chief Information Officer concurred with many of our recommendations, but did not believe that the bureau had placed sensitive information at an unacceptable risk for unauthorized disclosure, modification, or insider threat exploitation. He cited significant strides in reducing risk since the Robert Hanssen espionage investigation….

> (U)ntil the bureau fully and effectively implements certain information security program activities for the network, security controls will likely remain inadequate or inconsistently applied.

Misuse of computing resources follows a similar logic: wrongdoers will attempt only those things that they feel they can achieve.

Benjamin Robinson, a former agent for the U.S. Commerce Department, for instance, was indicted by a federal grand jury late last month on charges that he used a government database to stalk and threaten the life of a former girlfriend.

More disconcerting still is the rise of government "fusion" centers used to gather data from many sources into integrated databases for intelligence and law enforcement officials. Such centers, which meld information from numerous sources both public and private, raise serious privacy concerns, in particular the likelihood that erroneous data could be introduced to such a process or accurate data be misconstrued. These centers were recently the subject of a hearing before the Homeland Security Committee hearing (http://homeland.house.gov/hearings/index.asp?ID=90.) There are as of today no laws in place to restrict the scope of activities of these centers, which should give your committee pause.

We, like you, remain concerned that the government's poor track record on security, combined with ongoing opacity of intelligence operations, will compromise the privacy and security of American citizens. The government's power is growing at a time of great peril both at home and abroad. We urge you to be vigilant for risks that accompany such expansion of governmental might.

Sincerely,

Ed Black
President & CEO

900 17th Street, NW Suite 1100 Washington, DC 20006 Tel: 202.783.0070 Fax: 202.783.0534