SENATOR LIEBERMAN
THE GOVERNMENT SECURITY INFORMATION ACT OF 1999
HEARING STATEMENT
March 2, 2000

Thank you, Mr. Chairman, and thank you for calling this hearing on a topic of enormous concern to all of us. The security of our digital information is something that affects every one of us on a daily basis and should be taken as seriously as the security of our personal property, our neighborhoods, our communities, our nation, and in the worst case, the security of our lives.

The reach of the Internet and the alacrity with which it has achieved that reach is the story of the closing years of the 20th century. Enabled by the remarkable innovation in information technology, we are fast approaching a time when the world will always be on, always connected, always open for business. It will be a fast environment, marked by increasing efficiency and decreased cost. But it will also be intensely competitive and without boundaries. Almost every institution we rely on in our daily lives is feeling the effect of this latest technological revolution, from business to law to finance, and most certainly government.

Just last month, the General Services Administrations Chief Information Officer, Bill Piatt, wrote something all of us in government should keep in mind. He said, "From the perspective of our bosses - the citizens - the electronic government is neither an option to be chosen nor a mandate to be decreed. It is simply expected."

So, the basic goals of e-government - which are the electronic delivery of information and services - are the same as government's goals have always been, as enumerated in the Constitution. But if government is going to be plugged into the networked world, as an active, permanent presence, we will first have to protect the confidentiality, the integrity and, of course, the availability of the information contained on government computers. We must be acutely aware of the information at stake here. It covers everything from the movements of our armed forces and the deployment of our most powerful weapons, to accumulated data about the economy and the financial markets, to support for our transportation networks, to the most private information about the American people, such as tax, wage, and medical records.

This information, in far too many cases today, is wide open to exploitation - from pranksters to terrorists and every disaffected person in between. It is unacceptable that the GAO has labeled as "high risk" virtually the entire computer security system of our government. We must take action to take the government security of computerized information off the "high-risk" list.

Last year, the Chairman and I looked into what went wrong in the federal investigation of Wen Ho Lee, the former Los Alamos Nuclear Laboratory scientist indicted for downloading classified information to an unclassified computer. The Justice Department is still investigating, and Mr. Lee's guilt or innocence has yet to be determined. But the case should focus everyone's attention on the vulnerability that comes with reliance on computers. So too should the revelations that former CIA Director John Deutch maintained sensitive information on his home computer. The hacking of government sites, including those at the Senate, the FBI, the White House, Interior and the Department of Defense, is becoming a near daily occurrence. And I wouldn't be surprised if scores of other government sites have also been invaded - but we'll never know, because monitoring intrusions, much less reporting them, is not comprehensive.

There are many reasons federal, computer-based information is inadequately protected. But the underlying problem, according to GAO, is poor management. In some ways, this is a "cultural" problem. Our concentration on security simply hasn't grown at the same pace as our reliance on computers. The **Government Information Security Act of 1999**, which the Chairman and I have introduced, is a beginning step toward correcting this fundamental shortcoming. The bill would put every government agency on notice that it must implement a computer security plan which will be subject to annual,

independent audits, report unauthorized intrusions, and provide security awareness training for all its workers.

There are a number of areas we have not yet addressed in our bill, and we will be asking for input on how best to handle them. For example, the government needs to increase dramatically the number of trained information security professionals. In that regard, I'm intrigued by the President's proposal for a federal Cyberservice at Universities, based on the ROTC model, and we need incentives for universities to train more people in this area.

We will also need to consider what to do to keep the government informed of technological changes in computer security, so that we don't fall behind. The President's proposal to establish a national institute for computer protection sounds like a good idea, if it provides assistance with research and development and technical support.

So, Mr. Chairman, I am hopeful that our proposal will stimulate significant debate and early action. Our bill is a work in progress and we anticipate hearing from a broad swath of interested parties. We must particularly listen to those in private industry who have made, I think, much more headway than we in the public sector have in this area. We don't need to re-invent the wheel. We do need to share experiences and exchange ideas to learn what works best. I thank all our witnesses for appearing today and look forward to your testimony. It will help us craft the best possible legislation to secure the government's vast and important treasury of information.

Thank you.