Testimony of

Professor Lance J. Hoffman
Computer Science Department
The George Washington University
Washington, D.C.

Before the

U. S. Senate Committee on Commerce, Science, and Transportation
Subcommittee on Science, Technology, and Space

April 24, 2002

Thank you, Chairman Wyden, Senator Allen, and other distinguished members of the Science, Technology, and Space Subcommittee. It is an honor to have this opportunity to appear before you today and to assist in your efforts to strengthen our nation's information infrastructure and improve our capability to respond and recover from terrorist attacks and other emergencies.

I am Lance J. Hoffman, Professor of Computer Science at the George Washington University here in Washington, D. C. I lead the computer security graduate program in computer science and the Computer Security and Information Assurance Graduate Certificate Program. This academic year, I taught information policy and information warfare courses to students of computer science, international affairs, political science, and other fields. In 1993, I founded the School of Engineering's Cyberspace Policy Institute to examine the relationship between the technical and other factors that affect security, privacy, and related aspects of computer and information systems.

I am a Fellow of the Association for Computing Machinery (ACM), the nation's oldest and largest professional society of computer scientists, educators and other computer professionals committed to the open interchange of information concerning computing and related disciplines. The ACM has 75,000 individual members, including active professional and student chapters in Oregon, Virginia, and most states throughout the nation.

To underscore the importance of today's hearing this statement has been endorsed by the ACM's Committee on Computer Security and Privacy and the U.S. Public Policy Committee of the ACM (USACM).

I appreciate this opportunity to comment on S. 2037, the Science and Technology Emergency Mobilization Act, and S. 2182, the Cyber Security Research and Development Act, two significant pieces of legislation designed to address our nation's information assurance needs.

S. 2182

First, let me address S. 2182. This bill takes important steps to develop the cadre of scientists, engineers, and computer specialists who understand current information assurance problems and can ameliorate them while also developing long-term solutions based on improved, smarter technologies. To date, despite the fact that an increasing amount of daily life involves reliance on computer systems and networks, there is a remarkably small amount of long-term, ongoing funding available for computer security and information assurance research and development designed to solve these problems. This bill may remedy these concerns by providing the incentives and human resources necessary to meet some of today's security challenges and to take on tomorrow's. It does this in several ways, notably by the new research and education programs it calls for at the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST).

These programs will promote more innovative research in information assurance by attracting technically competent researchers into this field of national need. The bill is written in such a way that everyone from a senior faculty member wishing to focus his or her attention on computer security to a bright undergraduate student will be encouraged to work in this field. It will help to address the critical shortage of PhDs and graduates in the security field that limits opportunities for research and solving the critical challenges we face.

Computer security and information assurance have had trouble in the past competing with more established disciplines. Students and faculty have been driven by available funding opportunities to work on problems that are better known and whose solutions are in some cases more developed, but less important and critical to the nation than the security of its infrastructure. This bill will help to remedy that situation.

I especially like the inclusion of privacy and risk analysis as important areas of study, in addition to what some might consider more purely technical areas. Since innovative technical solutions developed in a vacuum without taking into consideration the surrounding constraints related to politics, cost, and legal liability will fail, the inclusion of these areas will guarantee that the pure technological solutions that come out of the programs that this bill funds will actually have a good chance of being implemented, working, and ultimately improving the security of the nation's infrastructure.

I also appreciate the foresight of the bill in recognizing and supporting not only traditional undergraduate and graduate fields of study, but also certificate programs in the area. I direct a certification program where working professionals come in after a full day at work, and devote an additional five hours toward a certification in security and information assurance. In the program we have just started, more than a quarter of the students have been motivated to go back to school and pursue more advanced master's and doctoral studies in this area, and to apply the graduate credits earned with their certificate to those higher degrees.

The bill is excellent as written, but the Committee may wish to consider a couple of minor changes that would improve it even further. For instance, it currently provides funds for faculty retraining in this area. But in many cases, this may not be a viable option since many universities are stretched thin in trying to properly cover the currently recognized core areas of computer science. It is hard enough to get established faculty members in one field to change specialties, and recruiting across departments is almost impossible.

There are only a limited number of faculty members in the U.S. who have significant background in security research. As my colleague Professor Eugene Spafford of Purdue University pointed out in his testimony last fall to the House Committee on Science, an informal survey of 23 preeminent U.S. universities with information security programs found that they graduated a combined total of 20 PhDs in security over the last three years. As you can imagine, there is an intense competition for the even smaller number of graduates interested in a faculty position. Explicitly allowing funds for faculty recruitment from outside (for example, from retiring Federal government and contractor security experts who have appropriate credentials, teaching skills, and the motivation to work as part-time or full-time faculty but would not otherwise have the opportunity) might provide another solution to this problem of building up the training cadre more rapidly.

While I am very encouraged with the funds authorized by this legislation, I would also suggest that program managers at NIST and NSF be allowed a bit more discretion in funding extraordinary projects with high risk and high potential. Setting aside a small percentage of the funds of this bill for small, innovative projects that address evolving and emerging research issues will allow researchers to, for example, fund a planning workshop or to encourage an add-on specialty day at an existing conference without a lot of red tape. These opportunities for research and information dissemination may lead to new innovative solutions and other advances in information security.

My final remark on S. 2182 relates to the requirement for placement data in fields related to computer and network security. A study of potential enrollment and placement for students enrolled in a proposed computer and network security program may be hard for many universities to generate at the same time they are starting these programs and assimilating the additional students generated by this and other programs. As a result, the development and growth of these programs could be unnecessarily impeded. I respectfully suggest that universities be allowed to concentrate on curriculum development and student recruitment up front. If you wish, universities could be required to collect appropriate placement data from students as they go through and exit the program. But requiring this up front is counterproductive.

S. 2037

Turning my attention to S. 2037, the Science and Technology Emergency Mobilization Act, I wish to commend the members of this Subcommittee for their noble attempt to harness the outstanding capabilities of our nation's science and technology community,

especially in times of national crisis. Faced with the realities of September 11, many members of the computing community wished to provide their technical assistance towards safeguarding our nation's infrastructure and in recovering from the attacks. S. 2037 would provide opportunities to match security experts where their services are most needed.

I wish to offer the following recommendations to build upon the many fine provisions of S. 2037. First, in establishing pilot programs aimed at achieving the interoperability of communications systems used by emergency response agencies, it is also necessary to achieve the integrity, assurance, and security of the communications. In attempting to improve emergency communications, it would be shortsighted to sacrifice security to achieve utility, particularly if it leads to vulnerable emergency communication systems. Wireless standards, where they exist, are known to be weak. Standards bodies, including NIST, should work to develop better wireless standards to ensure security and utility of such systems.

While the legislation takes necessary steps to require expertise checks, it lacks similar safeguards requiring background checks. This vulnerability might allow the introduction of technically competent malevolent individuals into risk equation. If we don't verify both the technical credibility and the personal background of individuals, we risk doing more harm than good.

Authentication precautions and other security mechanisms, combined with privacy policy guidelines, will be necessary so that if and when utilized, the "virtual technology reserve" database is only used by those responsible and is not misused (e.g., by an enemy attacking using a form of information warfare and polluting the database or identifying and harassing or impeding the responders identified therein).

The database will need to be designed and tested properly; possibly using competing designs with rapid prototyping. Both database and security experts should work on system design to insure appropriate access and security balances, speed of responsiveness, update ability, and accuracy.

While S. 2037 will help our nation respond to acts of terror and other emergencies, we must simultaneously engage in a more proactive approach that focuses on prevention. "Emergency prevention and response" is stated as an objective but it is much easier to demonstrate response than prevention [it's hard to have a demonstration if nothing is happening].

Chilling Effects of the Digital Millennium Copyright Act

One last but critical point that I wish to leave you with is that laws like the Digital Millennium Copyright Act (DMCA) inhibit the ability of individuals to engage in critical research in computer security and related fields. Unfortunately, this has certain implications for national security. For instance, researchers who study or teach encryption, computer security, or otherwise reverse engineer technical measures and who report the results of their research in this area face new risks of legal liability under the

DMCA. As University of California at Berkeley Law Professor Pamela Samuelson has noted, the limited exemptions carved-out in the DMCA have been found to be of little value to the research community. I encourage you to re-examine laws that prohibit or restrict computing technology instead of undesirable behavior. DMCA-like restrictions have the potential to cripple the very security advancements S. 2037 and S. 2182 are intended to advance.

In summary, I commend the members of the subcommittee for their legislative efforts to enhance the security of our nation's infrastructure and our ability to respond to national emergencies. Thank you for the opportunity to appear before you today. I would be pleased to answer any questions you might have.