

**George Strawn, Acting Assistant Director for
Computer and Information Science and Engineering
National Science Foundation
Before the Subcommittee on Science, Technology, and Space
Committee on Commerce, Science, and Transportation
United States Senate
April 24, 2002**

Chairman Wyden, Senator Allen, Members of the Committee, thank you for the opportunity to testify at this hearing on Homeland Security and the Technology Sector and the Cyber Security Research and Development Act. I am George Strawn, acting Assistant Director for Computer and Information Science and Engineering at the National Science Foundation. Prior to coming to NSF, I was a faculty member in a University Computer Science department and the director of an Academic Computation Center. As such I have been concerned about issues such as cybersecurity for a long time. As you know, the Administration has yet to take a position on S. 2182 so I will confine my comments to the need for cybersecurity R&D and provide you with an overview of NSF involvement in this important area. The Administration would appreciate an opportunity to analyze S.2182 and submit written views on it prior to the subcommittee's consideration of the bill.

Although cybersecurity has always been an important part of information technology (IT), over the last decade its importance has been greatly magnified. This is so because IT systems and services now are pervasive throughout society and because the Internet now ties together so many of our IT systems. While this interconnectedness of IT systems is enabling great productivity gains for the US economy, it has also enabled great gains for IT mischief makers and outlaws. Clearly, there is much understanding yet to be gained if we are to avoid unpleasant surprises and to foil those who would attack the internet or use it for illegal purposes.

Although the defense sector has always paid great attention to cybersecurity, the same cannot be said about many civilian applications of IT. Until recently, cybersecurity has been considered an "optional add-on" for many IT systems. As recently as two years ago, discussion at a President's IT Advisory Committee (PITAC) meeting indicated that the private sector "was not being rewarded" for cybersecurity products and services because they made IT systems more complicated and slower at a time when customers were wanting more simplicity and speed. Although these circumstances have begun to change, there is much to do before we will be able to achieve desired levels of cybersecurity.

Cybersecurity is now understood to be a rather difficult problem. This is true for many reasons, including that fact that cybersecurity is a property of the "total system", not of the system components (and those components include human and management elements as well as technology). This means that individually secure components and/or procedures can be put together to comprise a system that is not secure -- unless the proper attention is given to system-level security considerations.

Of course, the fact that the Internet makes “one big system” out of millions (soon to be billions) of component IT systems is a major source of complexity and insecurity.

Early research and development work on the Internet, as with many IT developments of the past, focused on “making it work”, not necessarily on making it secure. And because cybersecurity is a systems property, trying to add it on as an afterthought is very problematic. It would be much better to recreate IT systems with cybersecurity as a major design criteria than to attempt to patch it in after the fact.

Of course, we must and can attend to short-term needs and to long-term improvements simultaneously. Short-term cybersecurity patches are not only possible but are in progress throughout the IT world. In fact, a major challenge is to get cybersecurity services and procedures that have been developed over the last few years into wide use. Although there may be useful tactical contributions to cybersecurity that NSF can make (such as cybersecurity emphases in our Digital Government program), I would like to focus on longer term issues in cybersecurity because that is where NSF’s contributions can be the greatest.

As you know, NSF focuses on long-term fundamental research and education in all science and engineering disciplines. This long-term fundamental research has as its goal increased understanding of the subjects under study. And it has been the experience of science and engineering research that increased understanding leads to technology developments that are then put to important uses by society. In many cases the societal uses that result from scientific understandings were not apparent at the time the scientific work was being done. For example, important applications to cybersecurity may arise out of scientific research in IT systems (or even in other sciences) that doesn’t initially appear to be related to security. Nevertheless, there are important reasons to increase the emphasis on cybersecurity R&D as NSF has recently been doing.

NSF has supported cybersecurity research for a number of years, recently at a level of approximately \$20 million. A major problem in developing a robust cybersecurity research program is that the number of faculty members doing research in cybersecurity has been quite small. This is perhaps the most important problem to be solved as we seek to increase the amount of long term fundamental research in cybersecurity. Unless there is a sufficiently large-size community of cybersecurity researchers, there will never be a sufficient number of positions for graduate students to assist in the conduct of that research. This translates into a shortage of next-generation cybersecurity workers and faculty. It also means we will lack the courses and curricula needed to educate more students--undergraduates as well as graduates--ready to go into the cybersecurity workforce.

NSF’s Scholarships for Service/Cybercorp program is one way we are trying to address this issue. This program makes awards to qualified institutions to provide scholarships to undergraduate and graduate students studying computer security. In exchange, the recipients must serve in the Federal Government for at least two years. The program also provides capacity building grants to improve the quality and increase the production of computer security professionals. The program has been funded at approximately \$11 million the past two years and the Administration is requesting \$19.3 million in

supplemental funding to enhance this program in FY 2002.

Last September 5th, NSF announced a new research program, Trusted Computing, to focus our support for cybersecurity research. In addition to the estimated \$20 million that we anticipate as our ongoing investment in distributed cybersecurity research projects, we allocated an additional \$5 million for the Trusted Computing program. On December 5th, we received about 120 proposals in response to that announcement requesting over \$80 million of support. Our expert panelists who reviewed those proposals rated about 10 percent of them as “highly competitive” (high praise from the ever-critical research community) and rated almost half of them as worthy of funding. We will award funding to the highly competitive proposals. We believe that this program will motivate more faculty to turn their attention and expertise to cybersecurity. It will be necessary to focus attention on programs like Trusted Computing over the next several years if we are to help create a vibrant research community that will attack, and ultimately solve, many of the difficult problems associated with cybersecurity.

In addition to individual research awards, NSF has recently increased the number of large project interdisciplinary awards it has made in areas of IT research. Under the Information Technology Research (ITR) priority area initiated in 2000, NSF began a major invigoration of its IT research activities, including a focus on large, interdisciplinary research projects. We believe that this focus has already begun to show extremely valuable results by enabling computer scientists and engineers to work collaboratively on problems that require expertise from many areas to solve. I believe that many cybersecurity problems will also benefit from interdisciplinary groups or centers working collaboratively on their solutions. One important goal of fundamental long term research in cybersecurity will be to produce agreement on what, in fact, constitutes a secure system. When such an agreement is in hand, it will be possible to formulate important cybersecurity standards that, like all important standards, will facilitate their realization.

NSF also has considerable experience in supporting curriculum and academic program development and of administering graduate traineeship programs. Such activities could also help accelerated academic developments in cybersecurity as long as they are coupled with vibrant research support to attract the research faculty into the area as mentioned above.

NSF focuses on people, ideas, and tools as it pursues its goals of helping to keep the US in a world-leadership position in science and engineering research and education. Increasingly IT tools and services are required by all academic disciplines to achieve these goals. Therefore our efforts to contribute to cybersecurity research and development are increasingly required for our science and engineering community as well as by society at large. As IT continues to transform society, cybersecurity continues to increase in importance and is of increasing priority on our list of important scientific and engineering activities.

Thank you again for the opportunity to testify, and I would be happy to respond to any questions you may have.