Written statement of

W. Wyatt Starnes
Founder, President and CEO Tripwire, Inc.

Before the

Senate Sub-committee on Science, Technology and Space

Relating to
Homeland Security and the Technology Sector: S.2037 and S.2182

April 24, 2002

Good afternoon Mr. Chairman and members of the Committee. My name is Wyatt Starnes, a founder, CEO and president of Tripwire, Inc. I have followed with great interest the activities of the Federal government at this very critical time in our nation's history. I would like to commend this sub-committee, led by Senator Wyden and Senator Allen, and their staff, in directing focus on the critical issues of Cyber-risk and Cyber-security.

I appreciate the opportunity to present before this committee today.

For the past decade, the technology that is Tripwire has focused on data integrity assurance as a means to achieve higher levels of security, control, availability, and reliability of computing systems. Our focus has been on protecting critical computing infrastructure within the commercial and government sectors. Tripwire software has been deployed on hundreds of thousands of systems worldwide, including many inside of this building.

At Tripwire, we understand the importance of being able to rapidly detect, assess, and appropriately respond to threats, risks and even accidental changes to critical systems. Intrusions, computer viruses, logic bombs, hackers, "worm" programs, and badly written software can all lead to compromise, alteration and destruction of crucial information. Assuring the integrity and control of the ever-expanding digital infrastructure is crucial to our nation's financial viability as well as its safety and security. We understand that to fully manage the risks associated with maintaining information resources requires exerting positive control: our products enable that level of control.

It is as an information security professional and business leader -- as well as a citizen -- that I am here before you today to discuss the security and control of our nation's cyber-infrastructure, and why I have concluded that both Senate Bill 2182, the "Cyber Security Research and Development Act" and Senate Bill 2037, the "Science and Technology Emergency Mobilization Act" represent positive steps forward to safeguard our nation's somewhat fragile digital infrastructure.

Relative to Senate Bill 2182, our company understands the importance of supporting and funding research within the university system. After all, our core technology was initially developed at Purdue University almost ten years ago under the direction of Professor Eugene Spafford. We later obtained the commercial rights to the technology and have built upon the Purdue work to create high-quality, commercial data integrity assurance solutions that are in wide use around the world, including prominent usage within most branches of the US Government. Other fundamental information security technology, including security scanners, firewalls, VPNs, and intrusion detection systems all have roots in academic research at Purdue and elsewhere.

It is important to note that a considerable amount of this technology was developed without Federal support, and often without any external support at all. Research efforts over the last decade conducted at leading universities such as Purdue have been supported almost entirely by small corporate contributions. Unfortunately, there has been no Federal support for the kind of long-term and center-based research that is being conducted. We can only speculate at the solutions we might have in hand for today's problems had these researchers been supported at a more appropriate level.

Because of market pressures, including the recent economic downturn, industry support for leading academic programs with long-term vision has suffered. This scarcity of dollars has reduced the capacity of most academic programs, and may even threaten the existence of a few at a time when we are beginning to realize their importance. The small quantity of funds available, and their dominance by industry, tends to cause researchers to focus on "quick fix" patches instead of more fundamental solutions to society's cyber-weaknesses.

Consider:

- There are too few students studying cyber-security needs and issues;
- Too little is being spent to drive the technological research required to fight a war on the cyber-battle ground;
- There are too few researchers advancing the state of technology within the university system.
- There are not enough trained professors to develop and teach the courses to train a new generation of information security professionals.

Unless something significant changes, these problems may continue or worsen despite the best efforts of those of us working in cyber-security.

It is also necessary to provide mechanisms to allow public universities to accept equity from private industry in order to effectively capitalize on technology developed with public funding. Some states, including Oregon, currently limit or prohibit these transactions. Oregon is moving aggressively to remove these restrictions with a ballot initiative to change the states constitution. This effort has been largely driven by the private sector. We urge other states to begin the

important processes to reverse restrictive provisions relating to technology transfer by and between public Universities and the private sector.

We support Senate Bill 2182 as it provides a means to address these issues by creating and funding programs to stimulate new cyber-research and development. This should help to "prime the pump" enhancing our ability as a nation to stay ahead in the development of critical cyber-protection technologies.

There is no doubt that leading firms such as Tripwire will respond to immediate security needs by government and society at large. But we also believe it is vital that government take a role in ensuring that the creative minds in leading universities such as Purdue have the resources to work on the solutions we will need a decades from now, too.

Does this solve all our problems? No. The problem extends beyond university funding. We must enhance the coordination among state and Federal Government, the academic community, and private industry.

From my perspective as the CEO of a commercial company, we routinely see the desire and need for government and commercial entities to enhance their security processes. In many cases, especially within the government sector, the requirements to 'upgrade' critical systems come months or even years before the funding becomes available. It is in these critical gaps that our cyber-vulnerability as a nation is the greatest.

I urge the Congress to be aware of these gaps. Somehow, we need to find ways for government to operate in "Internet Time" when faced with bridging these gaps and expedite approvals and funding to address them.

Another area I would like to comment on are the issues of National and local coordination and cooperation. During the aftermath of the events of September 11, we've all heard stories of companies and organizations with the desire and expertise to help Government agencies. However, they found there were limited cross-agency mechanisms to coordinate this interest and well-intended response.

I am convinced we should learn from these experiences as the same sorts of challenges exist when dealing with threats and incidents of a "cyber" nature.

This leads me to offer my comments on Senate Bill 2037, the "Science and Technology Emergency Mobilization Act". I believe that this legislation can help by establishing a structure within the "National NetGuard" framework to enable the public and private sectors to work together more effectively when cyber-events threaten our country's electronic infrastructure.

This act intends to create an organized process and control structure to allow private sector to provide the appropriate assistance in times of need, as well as a mechanism for the Government to quickly locate and request assistance from qualified individuals within the private sector.

These capabilities are useful to enable the country to react quickly and appropriately to cyber-security issues, particularly when they impact our national infrastructure.

While I am supportive of the concept reflected in Senate Bill 2037 I urge the committee to think and act carefully in defining who and how the NetGuard members are qualified and enlisted. We must be certain that the mechanism created to assist does not introduce new vulnerabilities, competitions, or confusion. The urgency to get this infrastructure in place must be tempered by the need to 'get it right'.

Within our great state of Oregon the Private Sector is marshaling its resources to address these gaps at a local level. The Oregon Regional Alliance for Information and Network Security, or RAINS, is a consortium of private and public sector organizations and individuals forming around the following mission:

- To contribute to US defense and Homeland Security by providing solutions to critical cyber-security problems, and

- To expand Oregon's cyber-security cluster, creating jobs, cultivating technical innovation and education, and improving the state's economy.

I believe that this model can be extended nationally and dovetail with the initiatives proposed in Senate Bill 2037. The Oregon RAINS project will be hosting Richard Clarke and other Federal officials in Oregon to present this project on June 5-6, 2002.

Comments on Homeland Security

What the committee is addressing today could be included under the rubric 'Homeland Security'. I think it important to remember that many of the weaknesses in our infrastructures that we are concerned about today were identified by experts in academia, industry and government decades ago. Those warnings were not heeded because they involved additional appropriations and regulation that were not seen as having an immediate effect. Thus, we are now faced with an urgent need and much larger economic and social cost to retrofit solutions -- including some of dubious effectiveness -- into everything from communication to transportation to power distribution.

Experts have likewise been warning for years that our information infrastructure is at risk and that insufficient investment is being made in research, education, and deployment of safeguards. I believe that proactively allocating and expediting significant funding to enhance our National digital infrastructure before there is a major breach would be very prudent.

Summary

In summary, I am in strong support of this important legislation as it enhances the underpinnings required to address many of these obstacles and challenges. It will enable us to work together more effectively to improve our cyber-security capabilities, as well as ensure that we continue to advance the state-of-the-art with regard to protecting our cyber-infrastructure.

Thank you and I welcome any questions from the committee.