



Statement  
of  
Duane P. Andrews  
Corporate Executive Vice President  
Science Applications International Corporation (SAIC)  
before the  
Joint Economic Committee  
Hearing on The Wired Economy:  
Cyber Security and the U.S. Economy

June 21, 2001

Mr. Chairman and members of the Committee, I am pleased to be able to support your examination of cyber security in the U.S. economy. This is a difficult, multifaceted challenge. This morning I'd like to briefly highlight a few of the major issues related to cyber security that I believe require attention and that you may wish to examine in greater detail.

For perspective, I have been involved with cyber security matters for some time both in government and in industry. Currently SAIC provides support to the Department of Defense and several civil agencies, including supporting the FEDCIRC Incident Reporting and Handling Services, as well as commercial firms. We developed and still have an interest in a commercial security firm – Global Integrity – that created and operates the first Information Sharing Analysis Center, or ISAC, for the financial services industry – as well as ISACs for global firms and for Korea. I personally am active with the Industry Executive Subcommittee of the National Security Telecommunications Advisory Committee, commonly known as the NSTAC. In 1994 and 1999, I was a commissioner on both of the Secretary of Defense/Director of Central Intelligence-sponsored Joint Security Commissions that addressed cyber security, among other topics. I chaired the 1996 Defense Science Board Task Force on Information Warfare Defense. And as the assistant secretary of defense for C3I in the previous Bush administration, I initiated the Defense Information Assurance Program and the Department's information warfare program.

In the seven years since the first report of the Joint Security Commission, which included the observation that “the security of information systems and networks [is] the major security challenge of this decade and possibly the next century and ... there is insufficient awareness of the grave risks we face in this arena,” there has been progress. ISACs are enabling some industry sectors to share information on cyber threats. Presidential Decision Directive 63 organized efforts to address the critical infrastructures of the United States, and similar efforts are underway in several other countries. The Department of Defense has established a Joint Task Force for Computer Network Defense and has assigned operational control to USCINCSpace. Firewalls are in

widespread use and there has been modest improvement in training the work force on how to react to cyber events like viruses.

However, in my view, the rate of progress has been slower than the growth of the potential threat, and overall we have lost ground. A number of nations are developing information warfare skills; technology has gotten more complex; we have had deregulation of the telecommunications industry and are entering an era of converged services for voice, video and data; and, our commercial software packages are so large and complex that we cannot be sure what they contain. Further, the Internet has gotten too big to monitor effectively. In May of this year there were over 122 million Internet hosts, and the University of California at Berkley estimates there are 550 billion web-accessible documents, growing at 7.3 million pages per day. And in the next one to two years English will no longer be the dominant language of the Internet as much of Asia comes on line.

The failure to act is another major contributor to why we have lost ground. For a decade we have had study after study and report after report pointing out that our economy and our national security depend on the flow of information and that this flow is at risk. Numerous scenarios have suggested that the interconnection of systems and cascading effects can result in major disruptions to our economy and our national security systems.

These studies have also shown that we don't have to spend the gross national product or wait a decade to significantly improve our security posture and that we can take sound steps to protect systems and networks without trampling on civil rights.

So the question is: why haven't we taken the necessary steps to address the cyber threat? I can think of four factors that contribute.

- One: this is technically complex and hard to understand – a high geek factor – and that makes it hard for policy makers to engage.
- Two: every dollar that would go into protection, detection and reaction is a dollar that comes out of some mission or business function.
- Three: there is no oversight mechanism that holds federal agencies and critical business functions accountable. And,
- Four: we are treating this as a tactical, not a strategic problem.

To amplify, I'll start with critical infrastructure protection. This effort traces its legislative roots to Section 1053 of the National Defense Authorization Act for Fiscal Year 1996, entitled Report of National Policy On Protecting the National Information Infrastructure Against Strategic Attacks. This was known as the Kyl Amendment after its sponsor, Senator Kyl.

This legislation called for the President to submit to the Congress a report setting forth the results of a review of the national policy on protecting the national information infrastructure against strategic attacks. The report was to address the national policy and architecture governing the plans for establishing procedures, capabilities, systems, and processes necessary to perform indications, warning, and assessment functions regarding *strategic attacks* [emphasis added] by foreign nations, groups, or individuals, or any other entity against the national information infrastructure.

Subsequently, the President's Commission on Critical Infrastructures was established and the commission delivered a report entitled Critical Foundations Protecting America's Infrastructures. The recommendations in the report led to the creation of the National Infrastructure Protection Center (NIPC) and related activities. In my view, the commission and its report did not fully come to grips with preparation for strategic attack as called for by the Congress but rather turned to more tractable tactical matters.

In April of this year the General Accounting Office released a report [GAO-01-323] entitled Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities. While highlighting some progress in investigation and response support, the report notes several areas that need attention, particularly in aspects of national security.

I understand the current administration is addressing the government's critical infrastructure protection strategy and the specific requirements of the NIPC and hope they fully address the challenges and shortcomings identified by the GAO.

The decision to place the NIPC in the Justice Department led to law enforcement assuming the role as the front line of cyber defense. Once again, this focused efforts at the tactical level. Today, by default, the NIPC considers a cyber intrusion to be a crime. This has led to a lot of focus on hackers and on computer viruses. Clearly these activities require attention, but I do not believe they rise to the level of a strategic attack on the national information infrastructure.

This is not to fault the important work or dedication of the law enforcement entities as they fight crime in the cyber arena. It is just that law enforcement is not a sufficient response to this strategic challenge. More importantly, because of this tactical focus, as a nation we are not addressing the architectural strategies and recovery capabilities that can both deter and ensure we can recover from strategic attacks.

The Defense Science Board Task Force on Defensive Information Operations, 2000 Summer Study, March 2001, notes "Current policies and legal interpretations at the NIPC, the FBI, and the Justice Department ... have prevented timely and effective information sharing about potential national security risks."

Today there is no effective process in place to rapidly shift from a law enforcement posture to a national security posture. Nor is there a coordinated effort to be able to rapidly restore vital functions that are essential to the national defense or to the national economy.

These are areas that require attention. The Department of Defense should be required, and empowered, to take all appropriate steps to engage and repel intruders from its computers and networks without having to first resort to the criminal justice system. When warranted by circumstance, the DoD should also be prepared to participate in the protection of networks of critical importance to the national economic security. Maintaining an agile, robust, ability to defend the nation must have priority over criminal prosecutions.

Let me briefly turn to accountability. For over ten years the federal government has promulgated sound information security policy in OMB Circular A-130. If this policy had been followed over the years the protection of information in the government would be in much better shape than it is today. I suspect industry would have followed the

government leadership and also improved its security posture. However, I am unaware that anyone has been held accountable for not following that clear policy.

The Congress addressed this lack of accountability with the enactment of the Government Information Security Reform Act as a part of the FY2001 National Defense Authorization Act. The Security Act directs heads of agencies to identify, use, and share best security practices and to develop agency-wide information security plans, and to ensure sufficient protection “commensurate to the risk and the magnitude of harm that could result.”

I applaud the Congress for this legislation and urge the Congress to provide strong oversight to ensure this legislation is followed in letter and spirit and not just given the lip service that has been the case for the past decade. However, I expect that we may see some interesting interpretations of “risk” and “harm” as agencies attempt to avoid reallocating funds for information protection.

Another major challenge that requires attention is the sharing of information about cyber incidents between businesses, between governments, and between the government and business and academic entities. The GAO report I cited earlier reports some progress in this area but notes that many challenges remain. I urge both government and industry to more freely share information that reveals cyber weaknesses. I understand legislation is being considered to protect information exchanges on cyber incidents between industry and government from release under the Freedom of Information Act and to provide some antitrust protection to information sharing on cyber threat within industry groups. Such legislation would be a useful step.

Most importantly, I believe we must begin to address cyber and Internet issues from a broad, strategic point of view, not get overly focused on the equities of any particular government constituency.

In conclusion, I believe we need to take a fresh look at the challenge of a strategic attack through or on the nation’s cyber infrastructure. I believe the federal government needs to better clarify the issues and better characterize the strategic threat for the private sector.

This concludes my statement. I would be pleased to answer any questions you may have.