Testimony
to
Congress of the United States
House of Representatives
Committee on Government Reform
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census

Defining Federal Information Technology Research and Development:
Who? Where? What? Way? and How Much?

Focusing on
how investments in Information Technology
serve to protect this Nation and
position the US as a leader in the Information Technology arena.

Stephen L Squires, PhD

Hewlett-Packard Company
Chief Science Officer
Vice President

July 7, 2004

This testimony and associated statements are
based on my personal expertise and experience
and is not necessarily the official position of
the Hewlett-Packard Company

Executive Summary

Introduction

Thank you for inviting me to testify.
I consider it an honor and privilege to be here to discuss these critical issues.

My name is Stephen L Squires. In the private sector, I am the Chief Science Officer of the Hewlett-Packard Company. I am also a Special Government Employee (without compensation) Expert Consultant for the Department of Defense though the Defense Advanced Research Projects Agency. In this role I am a member of the Intelligence Science Board and also served on the Defense Science Board Task Force on Defense Roles and Missions for Homeland Security and other special working groups.

My testimony today is based on my own experience and expertise and does not necessarily represent the official position of HP or any other organization.

I will focus on what I believe is the most important issue identified in the letter requesting my testimony on the role of Federal investment in IT R&D.

> **Quote** *We also are interested in discussing how these investments [in Information Technology] serve to protect this Nation, as well as, position the US as a leader in the information technology arena.* **End**

My answer to this critical question is based on my understanding of the history of IT, my own direct experience and expertise in the most advanced research and development and applications focused on the most challenging problems facing the Nation, and my vision for the future.
My testimony is organized into four sections.

- A brief reference to history
- My own experience and expertise
- My Perspective
- Alternative Futures

A brief reference to history

The best way I can think of to start is a brief reference to history is the article titled “As We May Think” by Vannevar Bush in July 1945. The article was written in his role as Director of the Office of Scientific Research and Development, coordinating the activities of some six thousand leading American scientists in the application of science to warfare. He presents an extraordinary vision filled with a multitude of interesting examples including some in information technology. For example, he describes a system called “memex” that is essentially the Internet with a web of linked objects.

> The URL for the article is
> <http://www.theatlantic.com/unbound/flashbks/computer/bushf.htm>
> and can be accessed on the Internet using a standard browser.

The history of modern Information Technology is dominated by fundamental devices from the invention of the transistor, the integrated circuit, and the microprocessor along with other devices for the past 50 years. An extraordinary collection of systems have been developed though multiple layers of modules and structures to support a wide range of applications. The general term that describes the existing system is the Internet.

Information Technology has become increasingly pervasive. It is hard to imagine life without IT. And, our National Defense and Homeland Security depends on IT in addition to our Critical Infrastructure.

My own experience and expertise

I was recruited by NSA as a freshmen undergraduate electrical engineering student where I worked in its most advanced communications and information technology advanced research laboratories. Those laboratories focused on the most challenging problems, pursued advanced research to develop potential solutions, and worked with mission organizations to develop actual solutions. The extraordinary people that I had the privilege to work with and learn from for over 15 years made major contributions to much of the Information Technology revolution until the early 1980s. The extraordinary Information Technology systems of NSA made major contributions to winning the Cold War.

I joined ARPA in 1983 where I contributed to the vision, strategy, leadership, and management of advanced computing systems architecture that produced the technology base and foundation for the Federal High Performance Computing and Communications Program in 1992 and its extension to the National Information Infrastructure. It may be of interest to note that I testified to advocate the proposed legislation that initiated that program.

During my career with DARPA, I continued to maintain a close working relationship with the Intelligence Community. And, I was often called upon to participate in special working groups focused on critical issues of maintaining or achieving strategic advantage through advanced Information Technology. In fact, it was during a particularly frustrating period with one these working groups that I developed a briefing titled “Breaking out of the ‘post-Cold War’ Syndrome” in March 2000. This briefing focused on the limitations of existing information systems and the need for a new kind that would enable trusted information sharing along with other advances to achieve strategic advantage.

I joined HP in mid November 2000 as the Chief Science Officer, a new position created to focus on fundamental issues of Information Technology futures.

Less then a year later …

On the morning of 9.11,
it is still painful for me to think of that moment
— a globally shared moment in time —
I was at NSA that day on the second day of a two day meeting.

I was a member of a special working group focused on certain advanced technology issues to achieve strategic advantage in the new world of the Internet.

In general terms, these issues are an important aspect of this hearing
when we focus on the role of Information Technology
in National Defense and Homeland Security to
"*protect this Nation, as well as,*
position the US as a leader in the information technology arena"
as raised in the letter inviting me to testify.

My Perspective

New discoveries and new application challenges affect the dynamic and rate of change of the system of science, technology, and applications. The US Government has had a critical enabling leadership role in accelerating the advanced research, development, and application of IT since its beginning.

While the academic and commercial activities are generally well known, the relationship with the National Security Establishment is not because attention is normally deferred to the civilian departments, administrations, agencies, and organizations. The major exception to this is the Defense Advanced Research Projects Agency (DARPA) created as ARPA by President Eisenhower shortly after the launch of Sputnik. The DARPA focus has been and continues to be on advancing the frontier of science and technology in areas critical to the Defense mission. DARPA has had and continues to have an extraordinary impact on IT and related technologies.

The DARPA model is so successful that it serves as a model for others. We can only hope that the new HS ARPA in DHS is able to achieve its expectations. There is a similar kind of organization operating in the Intelligence Community. These are working together, complementing each other, building on each other's results, reducing risks, and accelerating technology transition. These investments also work to complement those of the National Science Foundation. The mission agencies also have their own research and development programs that work with the others in an effective complementary way including the National Laboratories. The collections of activities form an extraordinary system that has accomplished great things in cooperation with the academic and industry sectors.

Most of the work is done in the open. Most of the results first emerge in the academic and industry sectors. Many of the results transition into commercial products that are used by all sectors including the national security sector. But the goals, strategies, tactics, and management are often motivated and guided by classified issues, challenges, and applications—applications by the earliest of the early adopters.

The challenges of World War II, the Cold War, and the post 9.11 era each have their own distinctive characteristics. In the post 9.11 era the power and potential of Information Technology is recognized throughout the global community communicating and collaborating though the Internet

— a globally recognized phenomena.

IT industry and its applications have become a multi-trillion dollar sector of the global economy that is recognized as enabling new global dynamics.

Information Technology has become a commodity. The larger IT companies claim to have multi-billion dollar research and development budgets. The White House estimates that 85 percent of the critical infrastructure is in the private sector with much of it dependent on commercial information technology.

Therefore, it is only natural for some people familiar with other technologies to believe that there has been enough US Government investment in the future of Information Technology.

Let me say now in the strongest possible terms that such a belief is fundamentally misguided and absolutely wrong to the extent of being dangerous.

Now let me explain in terms of the one sentence I referenced in the letter inviting me to testify today.

How investments in research and development on information technology

1. Serve to protect this Nation and
2. Position the US as a leader in the information technology arena.

The investments were essential when they were not well known and the results were not directly visible. In the past 10 years the results have become more visible as IT has become pervasive. This represents a fundamental paradigm shift that is unprecedented in its impact. But, IT is not a single paradigm shift itself. IT is really a complex collection of paradigm shifts. While most of existing IT that is in pervasive use has become a commodity, this is the result of decades of investment by a complex public private sector partnership. The result of this investment has served to protect the Nation and has positioned the US as the leader in Information Technology. The fact is that IT enabled the US to win the Cold War as a critical part of the National System though research, design, development, deployment, and management of those systems. At the same time, the commercial applications served to strengthen the economy and demonstrate US leadership in Information Technology.

The effect has been profound. IT represents the most dynamic of all technologies. The past 50 years, since the invention of the transistor and the integrated circuit, has produced extraordinary advances through public private partnerships. These advances emerged from a complex science technology policy economy dynamic that we are only beginning to understand. While much of it started in the US, it has become a global phenomenon.

The entire field has been through multiple revolutions and extraordinary advances have been made across a wide range of science and technology.

But, we are only really at the beginnings of a much longer process.

As the limits of what has become conventional commercial integrated circuit technology are reached, new technologies with revolutionary implications are emerging at the atomic scale in the form of nano-technologies. The new nano-devices can be integrated into new kinds of things including new kinds of nano-scale integrated circuits with extraordinary properties. The properties go beyond computing to include new kinds of storage, sensors, effectors, and new ways to interact with the physical world including biological.

The advances in devices will enable new kinds of modules that will be the units of replication in new kinds of systems. The challenges in creating the new kinds of systems and their implications will be extraordinary as will be their capabilities. The advances are expected to be as revolutionary relative to the existing Internet as the Internet was to the first computer 50 years ago. And, at the nano-scale we are able to operate at the intersection of fundamentally new kinds of interdisciplinary interactions.

While the IT systems of today have become progressively more pervasive, the systems are awkward and visible, difficult to use, not well integrated into the environment and society, not suitable for critical applications, and not capable of trusted information sharing -- not to mention the continuing geometric increase in vulnerabilities and incidents that occur every day on the Internet.

Therefore, it should be obvious that there is even more advanced research to be done and it is more critical then ever – particularly in the post 9.11 era. While there is a growing global market and industry, it tends to focus on the near term even with their own research and development programs.

The US Government has a Constitutional responsibility and obligation to protect the national interest by providing for the common defense and enable the life, liberty, and happiness of the People. Among all the technologies, information technology is among the most critical and pervasive.

Some examples of the role of IT

- The role of IT in Critical Infrastructure
- The role of IT in the National and Global economy
- The role of IT in Science and Technology
- The role of IT in National Defense
- The role of IT in Homeland Security
- The role of IT in Trusted Information Sharing
- The role of IT in Protecting Individual Privacy
- The role of IT in the Future of Civilization

Some insight in the advanced research challenges can be found by exploring the fundamental trends, limits, and alterative futures in the context of a 5 layer model that covers everything from the devices to the applications:

Devices
The fundamental devices and their integration into components that provide the foundation for modules

Modules
The scalable components and systems of components that provide the underlying hardware, embedded software, and system software that serve as the foundation for scalable systems.

Virtualizations
The virtual system modules that are configurable into extensible scaling systems that serve as the foundation for customizable system structure.

Structures
The system structures that serve as the foundation for composing dynamic extensible scalable applications.

Applications
The applications of a system to the environment outside the system including users, the real world, and other systems.

Alternative Futures

There are four major alterative futures that I call Red, Orange, Yellow, and Green in the context of an idealistic vision of the future, Blue.

Red is essentially pre-Internet technology.

This is legacy IT that was developed and deployed before the Internet revolution. This is the IT of the Cold War era.
The old world of IT called legacy systems that should be donated to the Computer History Museum.

Orange is essentially an attempt to extend the Red to cope with the emerging Internet revolution.

An attempt to extend the life of legacy systems trying to connect IT to the Internet.

Yellow is essentially an attempt to apply commercial Internet technology to the challenge of the Internet.

The Internet and its evolution.

Green is essentially the development of fundamentally more advanced technology then commercial Internet technology for the purpose of achieving Strategic Advantage. Such systems also have fundamentally more advanced cyber security then the existing commercial Internet.

The revolution beyond the Internet representing a collection of fundamental advances across the 5 system layers providing federated adaptive enterprises capable of trusted information sharing for critical and pervasive applications.

Blue is an idealistic vision of the future that is called Intrinsic Trust and that is the essential distinguishing characteristic of the fundamental advance needed in future of Information Technology systems.

In this framework, the existing Internet is Yellow as generally applied throughout most of the modern global community. The US Government systems span the Red, Orange, Yellow, range with selected special features to protect them through a combination of physical separation and advanced cyber security. The existing US Government systems are obviously not Green because it does not exist—yet.

The most challenging problems provide the insight needed to establish the most effective advanced research agendas. The ideal of Blue is essential to guide the advanced research agenda for Green.

The insights needed to create effective advanced research agendas emerge from interdisciplinary interaction among science, business, homeland security, and national defense. The interactions are more critical because of the need for the public and private sector systems to interoperate over a wide range of modes that are all dependent on critical and pervasive interoperable information systems capable of trusted information sharing while protecting privacy.

Therefore,

I believe it is essential that the US Government continue to
invest in advanced research in Information Technologies
focused on protecting this Nation, and
position the US as the leader in Information Technology.

The future leadership of the United States depends on advanced science and technology at a time when Information Technology has become critical and pervasive and is itself going through its own re-invention.