TESTIMONY OF JAMES ADAMS
CHIEF EXECUTIVE OFFICER
INFRASTRUCTURE DEFENSE, INC.

COMMITTEE ON GOVERNMENTAL AFFAIRS
UNITED STATES SENATE
MARCH 2, 2000

Introduction

Chairman Thompson, Ranking Member Lieberman, members of the Committee, good morning and thank you for including me on this distinguished panel. My name is James Adams and I am the CEO of Infrastructure Defense Inc. (iDEFENSE).

By way of brief background, iDEFENSE provides intelligence-driven products -- daily reports, consulting and certification – that allow clients to mitigate or avoid computer network, Internet and information asset attacks before they occur. As an example, iDEFENSE began warning its clients about the possibility of Distributed Denial of Service attacks – the kinds of hacker activity that is currently capturing headlines across the globe - back in October and November of last year.

At the outset, I want to commend Senators Thompson and Lieberman, and their respective staff, for crafting such thoughtful and badly needed legislation in the area of computer security for the federal government. We are currently in the midst of a revolution, the Information Revolution, which calls for dramatic and bold steps in the area of securing cyberspace. The old ways of doing business don’t work any more.

It is in this context that the Thompson-Lieberman bill takes a crucial step forward. By shaking up the current culture of lethargy and inertia gripping the federal government with a proposal to put teeth into the OMB’s oversight of computer security issues this bill is a solid step in the right direction.

Why does this matter?

Few revolutions are accomplished without bloodshed. Already, as we plunge headlong and terribly ill-prepared into the Knowledge Age, we are beginning to receive the initial casualty reports from the front lines of the technology revolution and to witness first-hand the cyberthreats that, if allowed to fully mature, could cause horrendous damage to society.

The ongoing campaign of Denial of Service attacks include some of the household names of e-commerce — Microsoft, Yahoo, eBay, Amazon.com, CNN, ZDNet, and E*Trade. Comparative newcomer Buy.com was attacked on the day of its Initial Public Offering, and other smaller firms such as Datek Online Holdings Corp. experienced problems, which are probably related to the attacks. Targeted sites receive hits on their servers of up to one Gigabyte of data per second, and are unavailable to the general public for anywhere from 30 minutes to several hours.

From the headlines, you would think that these attacks suggested the end of the cyberworld as we know it. Nothing could be further from the truth. These were mere pinpricks on the body of e-commerce. Consider instead that some 30 countries have aggressive offensive Information Warfare programs and all of them have America firmly in their sights. Consider, to, that if you buy a piece of hardware or software from several countries, among them some of our allies, there is real concern that you will be buying doctored equipment that will siphon copies of all material that passes across that hardware or software back to the country of manufacture.

The hacker today isn’t just the stereotypical computer geek with a grudge against the world because he can’t get a date. And not every hack that is successfully pulled off is as sophomoric as, say, a recent incident when the self-styled Masters of Downloading hacked into the official U.S. Senate Web site and replaced its front page with a message proclaiming “Screw You Guys.”

The hacker today is much more likely to be in the employ of a government, of big business or organized crime. And the hackers of tomorrow will be all of that and the disenfranchised of the 21st century who will resort to the virtual space to commit acts of terrorism far more effective than anything we've seen from the Armalite or the Semtex bomb in the 20th century.

Consider the band of Russian hackers who, over the past two years, have siphoned off an enormous amount of research and development secrets from U.S. corporate and government entities in an operation codenamed Moonlight Maze by American intelligence. The value of this stolen information is in the tens of millions—perhaps hundreds of millions—of dollars; there's really no way to tell. The information was shipped over the Internet to Moscow for sale to the highest bidder.

Fortunately, this threat was detected by a U.S. government agency. Unfortunately, that information was not passed on to the private institutions that it might have helped. Among government and industry alike, an understanding of the critical infrastructure's threat environment is barely in its infancy.

All of these attacks, mistakes, and plain acts of God need to be studied very carefully. Because they define the threat front that is driving right through our very fragile economic, governmental, and corporate armor.

These are the kind of problems we—jointly, the public and private sectors—face in the technology revolution. So the big question is, who is going to solve these problems? The government? Private industry? Or the two working together? Or are the problems going to be solved at all?

How has government responded so far? Well, there has been the usual President's Commission, and then the Principal's Working Group, then the bureaucratic compromise that nobody really wanted and then the National Plan which arrived seven months late and wasn't a plan at all but an invitation to have more discussions. Meanwhile, the government in all its stateliness continues to move forward as if the Revolution is not happening. Seven months ago, my company won a major contract with a government agency to deliver urgently needed intelligence. The money was allocated, the paperwork done. Yet it remains mired in the bureaucratic hell from which apparently it cannot be extricated. Meanwhile that same government agency is under cyber attack each and every day. This is not a revolution. This is business as usual.

Another government agency is trying to revolutionize its procurement processes to keep up with the pace of the revolution. They are proudly talking about reducing procurement times down to under two years. In other words, by the time new equipment is in place, the revolution has already moved on eight Internet years. In my company, if I can't have a revolutionary new system in place within 90 days, I don't want it.

What this means to me is that the threat is growing rapidly, that a largely inert government has so far been unable to meet the challenge and that more must be done. And this does matter because there is more at stake here than simply whether a new computer works or does not, whether a web site is hacked or not. At stake is the relationship between the governed and their government in a democracy. High stakes indeed.

So, I welcome the Thompson-Leiberman legislation as a good first step in the Senate efforts to try and control and drive the process that will bring the government up to speed with the revolution. I believe, however, that to effectively cope with the technology revolution, this proposal must be strengthened a great deal.

To fix the problems that afflict our body politic and our body corporate will require far more than Band-Aids. We're not talking casts and splints or even organ transplants. What we're talking about is leaving the old body and moving into a new one. We are talking—I am talking—about beginning to make changes in our cultural, political, and economic processes and institutions of such magnitude that they will dwarf even those that accompanied the industrial revolution.

What is needed is an outside entity – with real power – to implement drastic change in the way government approaches technology and the underlying security of its systems. Currently, jurisdictional wrangling, procurement problems and a slew of other issues are seriously hampering governments ability to stay current with the rapid pace of the Information Revolution. The Thompson-Lieberman bill provides a framework to begin sorting through this mess.

However, what is needed most is a person or an entity that will draw on skill sets in many areas will overlap that of the CIO, CFO, CSO, and most of the other officers or entities. Let's give this new person the title of Chief of Business Assurance. Or perhaps the Office of Business Assurance to relate it directly to the federal government.

This new acronym should be the response to the current need. In some ways it is mirrored by the debate that started at the beginning of the Information Revolution that led to the appointment of Chief Information Officers in many companies and within government. But Business Assurance is more than security, more than technology, and more than a combination of the two. It is an understanding of the whole environment and what that means for a business or a public sector operation.

The OBA's task would be to continuously gather and synthesize infrastructure-related trends and events, to intelligently evaluate the technological context within which the organization operates, to identify and assess potential threats, and then to suggest defense action. Or, viewed from the positive side, to assess the technological revolution's opportunities and propose effective offensive strategies.

The Office of Business Assurance must be a totally independent organization, with real teeth and power within government. Those organizations that have the foresight to create and properly staff this position will be immeasurably better equipped to handle the tidal wave of change that is just now beginning to break over our government, industry, economy, and culture.

There is much in common between government and industry when it comes to the challenges—and the opportunities—that the technology revolution poses. Both sectors face a common threat that ranges from vandal hackers and hard-core criminals to foreign agents and natural disasters. Both sectors share common goals for the well being of America and her people. Both employ technologies that are in essence identical. And both must work together to protect each other.

My company, Infrastructure Defense, pioneers an approach to infrastructure protection that is aimed chiefly at the private sector. Many of the principles, however—value-chain analysis, for example, and threat analysis—are directly transferable to government organizations. The two sectors are not that far apart.

With common problems and common goals, there are opportunities for common solutions. One of the most important, I believe—one that is too new to have been embraced by either the private or public sector—is the need for every organization to incorporate a risk-mitigation process. A second priority is to build a comprehensive information sharing system across all sectors on cyberthreats and countermeasures. We cannot afford to allow important information to grow stagnant within particular public or private entities. The rapid pace of technological change necessitates a correspondingly robust response mechanism. I urge this Committee to champion this important issue as the federal response to the growing cyberthreat is constructed.

Conclusion

I leave you with this thought. You will see total transformations of the way business and government is conducted, internally and externally. A failure to change to meet these new challenges is to risk the destruction that all revolutions bring in their wake. Proactive action is the route to survival.

We have heard a great deal in recent months about the potential of a digital divide that is developing between the computer haves and the computer have nots. I believe there is another digital divide that is growing between the American government and its citizens. If this Committee's efforts do not move forward in changing the culture of inertia, there is real danger that the "digital divide" that exists between the government and the private sector will only widen. We cannot afford a situation where the governed feel that their government is out of touch and increasingly irrelevant to their lives. By stepping up to the plate and tackling computer security with an innovative, bold approach the Thompson-Lieberman bill significantly boosts the chances of reversing the current bureaucratic approach to a dynamic problem.

Again, thank you for the honor of appearing before the Committee today.