



## Remarks by Secretary Tom Ridge at the National Cyber Security Summit

For Immediate Release  
Office of the Press Secretary  
December 3, 2003  
\*\* Remarks as Prepared \*\*

Thank you for that introduction. It's an honor for me to be here this morning. I want to thank all of you for your willingness to be a part of this summit, and for your commitment to the protection of the cyber infrastructure that is so critical to our economic and national security.

I'm glad to see my friend General Gordon, I want to thank him and the President for their strong commitment to this important issue. At Homeland Security, we've got a great team at work protecting our physical and cyber assets...Bob Liscouski and Amit Yoran...thank you for all that you do to serve this country.

I want to especially thank the Business Software Alliance, ITAA, TechNet, and the U.S. Chamber of Commerce for their help in organizing this summit and for their strong support of our homeland security mission.

That mission...securing America against the scourge and scope of terrorism...is a challenge unlike any we have ever faced. An enemy that never rests, capable of obtaining weapons that come packaged in suitcases and envelopes, cars and cargo...

- 95,000 miles of shoreline to protect
- 7,000 miles of shared borders with Canada and Mexico to safeguard
- Thousands of tons of cargo to inspect
- And over a million people to process coming across our borders on a daily basis...

It can seem an impossible task.

Yet history teaches us that great things have been accomplished by those who pressed on in the face of the impossible. The Wright brothers proved flight feasible...America put a man on the moon...and not far from here Joseph Strauss constructed a bridge.

Due to many obstacles...enormous construction costs, constant gusting winds of over 60 miles per hour, swift ocean currents...Strauss was told it couldn't be done...his dream for many years was known as "the bridge that couldn't be built." But he persevered, and today we know his architectural marvel by a different name...the Golden Gate Bridge.

It's been said that "the only way to discover the limits of the possible is to go beyond them into the impossible." Those of you in this room are well acquainted with this truth. The very character of cyber technology and the Internet age has been defined by those who have gone beyond what is seen, who have tested the limits of the possible and in doing so have enriched our society and transformed our way of life.

Our cyber systems have connected us as a nation...as a people...as a global community in ways unimaginable even just a generation ago. And it is this type of connectivity that also defines our vision of homeland security.

It's a vision of shared leadership and shared responsibility. A vision that depends on all segments of our society...academia, citizens, local government, business...coming together around a shared goal of homeland protection.

As we confront the crucial issue of cyber security, it's important that our efforts follow a similar path...one where we share information, work together, and close any gaps and weaknesses that terrorists would otherwise seek to exploit.

The sheer reality is that we rely on computers. In many visible ways, the applications of computing are a part of our everyday life...e-mail, Internet research, online shopping. However there are countless other ways computers impact us daily that as a society we take for granted.

A vast electronic nervous system operates much of our nation's physical infrastructure. Everything from electricity grids to banking transactions to telecommunications depends on secure, reliable cyber networks.

These networks and the infrastructures they support present an attractive target for terrorists. They know, as do we, that a few lines of code could ultimately wreak as much havoc as a handful of bombs.

And the unfortunate truth is that the number of cyber-security incidents is on the rise. More than 76,000 occurred in just the first six months of this year. Many of these are the work of "hackers." Yet we know the enemies of freedom use the same technology that hackers do...that we do. And we know that they are looking to strike in any manner that will cripple our society.

So we must be as diligent and determined at finding ways to strengthen our cyberspace, as the terrorists are in trying to find ways to attack it. For every hacker or terrorist that tries to throw a worm or virus in our way, we must have effective roadblocks and tough barricades to throw in theirs.

And that's exactly what we are doing.

As the President made clear earlier this year when he released his National Strategy to Secure Cyberspace, the highest protection of our cyber security systems is one of the top priorities of this Administration and this new Department. And since the tragic events of 9/11, we have made solid progress in this area.

Before 9/11, industry, government, and even financial markets knew of our nation's increasing vulnerability to cyber terrorism, but our response lacked full coordination, focus, and resources.

Now, we have the National Cyber Security Division, as part of Information Analysis and Infrastructure Protection within Homeland Security, solely dedicated to the protection of our country's cyber assets. From the assessment of emerging threats...to the issuance of timely cyber security warnings...to our work with the private sector to address cyber issues, DHS's NCSD is providing strong cyber security leadership...portal to portal...network to network...all across this nation and in concert with nations around the globe.

We're fortunate to have Amit Yoran at the helm of this new division. He brings a wealth of cyber security experience from his time at Symantec Corporation and the Department of Defense. I join with the President, as well as our state, local, private sector and international partners in saying that he's doing a terrific job. Amit, all of us are truly grateful for your wise and dedicated leadership.

Let me also add that before 9/11, each separate sector of our nation's critical infrastructure had its own mechanism for sharing information, but there was no coordination between these different industrial sectors.

Now, the NCSD in partnership with Carnegie Mellon has created the U.S. Computer Emergency Response Team (U.S. CERT), which will provide a central coordination center to direct our response to any possible cyber attacks. In October, Homeland Security staged a "Livewire" exercise to simulate a cyber attack on computers, banks, and utilities. While, on the whole, the government response was successful, we found communication was not as smooth as it needs to be between the various sectors.

That's where the U.S. CERT comes in. It's charge is to ensure that the necessary information to repel an attack is distributed across all critical infrastructure sectors during a time of attack or heightened level of alert.

Additionally, the US CERT will work closely with the private sector and technology experts to enhance our warning and response time to a cyber attack - speed action when action is critical.

What else was lacking before 9/11? Well, frankly, the federal government didn't have a centralized method to communicate cyber threat warnings to the public.

And yet, now, through the U.S. CERT we will provide a range of information products with updates and reports on cyber vulnerabilities, as well as cyber security warnings that outline necessary steps to take in the event of a cyber attack.

From small businesses to large enterprises, from home users to owners and operators of critical infrastructures, all will be able to stay informed and improve security practices just by accessing the U.S. CERT website. This alert system is part of a larger, overall effort to raise public awareness about cyber threats.

After all, anywhere there is a computer...whether in a corporate building, a home office, or a dorm room...if that computer isn't secure, it represents a weak link. Because it only takes one vulnerable system to start a chain reaction that can lead to

devastating results. And that's why we must urge all Americans to take an active role in their own personal cyber security.

It's a message we're taking to the public. Through public education campaigns, public-private partnerships, and investments in groups such as the National Cyber Security Alliance and the Stay Safe Online program, Homeland Security aims to reach more than 50 million Americans in the next three years.

Of course, we recognize all these efforts for what they are...a good start...a good foundation upon which to build. And over the next few months, we will rigorously move forward to augment our cyber security capabilities.

But, as I've said many times before, the federal government can't succeed in these efforts alone. Eighty-five percent of our nation's critical infrastructure, including the cyber network that controls it, is owned and operated by the private sector. As such, we not only need businesses to be active partners with us in securing these vital assets, we need businesses...we need those of you here today to lead the way.

As we've seen time and time again, the expertise and insight of the business community is invaluable. Quick action and strong partnerships helped blunt the impact of the Blaster worm and SoBig virus...just as built-in redundancies and preparations by the private sector helped prevent loss of financial data during the East Coast power outage.

So, it should go without saying...the continued success of protecting our cyberspace depends on the investment and commitment of each of you and the businesses you represent.

The main purpose of this summit is to further strengthen the partnerships between Homeland Security and the private sector...to tap into the talent and ingenuity assembled here...to pick your brains as we work together to meet the challenges we face in securing our cyberspace.

The President laid out a vision, but what we need now is a blueprint...the practical steps we must take to realize that vision and our goal of greater security for our cyber networks and the physical infrastructures they support.

On a host of issues...raising awareness for home users, implementing a national cyber security warning system, creating more secure software...we need your input and your help if we are going to challenge the limits of the possible and strive toward a level of protection that will seem impossible and impenetrable to our enemies.

Unlike the great wars of the past, the war on terrorism is not fought solely by brave soldiers on far away battlefields. It is fought by border patrol inspectors who stand guard, firefighters and police officers who remain at the ready, moms and dads who prepare their families...it is fought by each of us.

So, again I want to thank you for your willingness to not only join with us today, but to further the work of your respective task forces in the coming months...to be a part of our mutual fight to protect our nation and our citizens.

Though the task of securing our homeland may at times seem daunting, it is not in the American character to back down before a challenge, to give in before a threat. We have not and we will not give way before the threat of terrorism.

As the passage of time renews our confidence, we can not let it weaken our resolve.

As the poet Henry Longfellow wrote, "Wisely improve the present. It is thine. Go forth to meet the shadowy future, without fear."

With each new day that dawns, we must meet it with the same sense of urgency, the same conviction of purpose, the same call to sacrifice we felt on September 11.

We must seize the moment given us...improve the present...so that the future we build is one where the shadows of fear and terror are held at bay by the light of hope and the promise of freedom.

Working together we will prevail. And we will win through to a day when that future will stand just as strong and secure as the bridge of Joseph Strauss.

A future that will stand for the same truth Strauss learned building his bridge...to press on in the face of adversity, to remain undaunted by the impossible...that determination is what transforms great dreams into a foundation for remarkable feats of accomplishment.

Thank you.