

**The Information Technology Association of America (ITAA)  
and  
the Center for Strategic and International Studies (CSIS)  
present**

**"Strengthening Homeland Cyber Defense"**

October 18, 2001  
9 am - 12:30 pm  
B1 Conference Center  
1800 K Street, NW  
Washington, DC

**Comments by John Tritak  
Director, Critical Infrastructure Assurance Office**

DIRECTOR TRITAK: I welcome you to the second half of this program on strengthening homeland cyber defense.

The purpose of this panel here is to hear the views of some leaders in the area of cyber defense and what needs to be done, going forward, in light of the events of September 11. I want to apologize up front. I'm going to have to leave shortly after the presentations are made here, and the Q&A session will be taken up by Jim Lewis and his colleagues from CSIS and ITAA.

But I would like to make a couple of opening remarks, just say a little bit about where things are going within the government, the role that our office and others play in this effort, and then turn the floor over to our panelists.

I suppose I could say without exaggeration that one could not say enough about the losses we all felt ?? suffered as a result of September 11. Speaking personally, one of my dear colleagues at the CIAO lost her sister at the Pentagon. And I know that one of our panelists here today lost a very dear colleague on one of the aircraft that was involved in the terrorist attacks.

You know, I've been called a number of times from press and colleagues and others, and they say, "What's changed now? What's so different about critical infrastructure protection after September 11?" And the urgency has not changed; the appreciation that there's an urgency has. Much of the work that we spend our time on at the CIAO in working with our colleagues and other federal agencies is to establish a case for action.

One of the cases for action was the concern that our nation's infrastructures are at risk from deliberate attack, whether physical or cyber. And whereas a good number of companies, and some of them are here today, have acknowledged that concern and were actually taking measures and actions to address that problem, the fact of the matter is the national security component of our policy was not self-executing in the market.

And we spend much of our time trying to demonstrate that, in fact, there's a business case, that it makes good business sense to do this, as well as helps contribute to our nation's security. I think it's fair to say since September 11 there is a very heightened awareness that national security is a business concern.

We all depend on our infrastructures to provide for the services that are needed to conduct our daily lives, to run our businesses, and for the Federal Government to meet its obligations under the Constitution.

Someone has asked me, "Well, how does critical infrastructure protection fit into homeland security? You know, what's going on here? Are they the same? Are they duplicative?" The answer is, as far as I can see it, is homeland security is about protecting all life and property within the borders of the United States. It's about protecting you and me against terrorist activity, whether we're at home, driving on the road, going to an airport.

Critical infrastructure protection is one component of that, assuring delivery of vital services over our nation's infrastructures to enable the government to function properly and to maintain an orderly functioning economy, and to provide the services that we depend on in our lives is an important of homeland security. But it's one part.

And I think it was quite proper ?? I noticed that the title is "Homeland Cyber Defense," which recognizes that the concerns for cyber defense are not limited to the protection of national infrastructure. They extend to all parts of our society and economy.

Now, clearly, the events of September 11th demonstrated that physical attacks against the United States are real and have been demonstrated and with horrific effect. But one thing I think we need to understand and what was demonstrated by September 11 is not that physical attacks are the way that terrorists are going to try and harm us.

The people that were responsible for this dastardly act are trying to undermine our way of life, and they're going to exploit vulnerabilities wherever they can find them. That includes exploiting whatever vulnerabilities may lie in cyber space or our dependency on information systems and networks.

That is why the President two days ago issued an Executive Order creating a Board for Critical Infrastructure Protection with a view towards focusing on the specific challenges of deliberate attacks on the nation's critical infrastructures via the information systems and networks that operate those infrastructures.

Clearly, the most serious and most immediate concern is the extent to which terrorist organizations can exploit cyber space to do their worst. But unfortunately, or fortunately as one would look at it, the information age has been very democratic in making available tools of disruption. They are not the sole monopoly of terrorist groups. They are widely available and being used by a wide range of potential bad actors, both international and domestic.

And also, the ability to exploit cyber space and leverage that exploitation to create significant disruptions in some cases cannot be understated, which is why this effort and this focus is a particular ?? being given particular attention within the administration.

But let's be clear about one thing. At the end of the day, we're talking about one coherent, holistic approach to defending the nation's homeland in which this portion, what I'm describing now, is one part. It's a division of labor issue.

To the extent that we're talking about homeland security, everyone reports to Tom Ridge, Governor Ridge actually. So going forward, we also recognize, as we did in critical infrastructure generally, but homeland defense more broadly, is that it can't be done by federal action alone.

Public-private partnering to defend the homeland in all its dimensions is a collaborative effort. And if one reads the Executive Order on homeland security that created the position for Governor Ridge, one will recognize throughout that document the need for collaboration.

Now, everyone realizes we need partnering, and partnering, in fact, has already been taking place. Over the last several years various partnering arrangements to address very specific problems and challenges to cyber defense, infrastructure assurance, and the rest, have been in place.

But we all acknowledge in light of September 11 that more needs to be done more quickly. And the administration recognizes this. This Board that has been created for critical infrastructure protection will coordinate across the major federal agencies all aspects of security and protection of national infrastructure in the information domain.

In addition, there will be members of the Board who represent interagency organizations who have particular expertise in critical infrastructure protection, including the Critical Infrastructure Assurance Office. I have ?? and of course, Ron Dick, who I think may have left ?? is also represented there.

So the team has been put together and now the need to go forward is at hand. We recognize that we need ?? the government can actually play a very important role in facilitating market solutions and voluntary actions which actually help support and secure the nation's infrastructures, information sharing being one of them.

And one call that has been around for several years, which is now going to be acted upon, is the need to be able to safeguard information that's shared with the Federal Government under the Freedom of Information Act.

And the administration has decided that it would support a narrowly-crafted FOIA exemption to safeguard information sharing with the government for the specific purpose of defending against hackers or deliberate attacks against information systems and networks via cyber space.

And, of course, you heard today Senator Bennett, who is one of the architects of one proposal to do just that. There are others, including one from Congressman Davis, that are being looked at as well.

I am confident that our work with the Senator and the Congressman will produce an exemption that's narrowly crafted, tightly honed, and is fully protective of open government and privacy.

Now, it's my pleasure to introduce the panel we have before you today. One of the first things we learned in government about partnering is sometimes it's better just to shut up and listen to people who know what they're talking about. And I am about to follow my own rule.

Our first speak will be Steven Blumenthal, Senior Vice President and CTO of GENUiTY. Our second speaker will be George Conrades, Chairman and CEO of Akamai Technologies. Our third speaker will be David Langstaff, CEO of Veridian Corporation. Our fourth speaker will be Gail Phipps, Executive Vice President of CACI International. And our final speaker will be Dr. Ernst Volgenau ?? Volgenau?

PARTICIPANT: Close enough.

DIRECTOR TRITAK: I only practiced all night on this, and I still screwed it up.

(Laughter.)

In his case, it's a big name.

Anyway, they will all speak sequentially for approximately five to eight minutes, and then after all of the speakers have given their opening remarks the floor will be open to questions and answers.

Thank you very much. Steven?

(Applause.)