Remarks prepared for

Deputy Secretary of Transportation Mortimer L. Downey

for Delivery during the

Transportation Research Board Panel
Challenges to and Developments in Critical Infrastructure Protection
Monday, 8 January 2001, 1:30 - 3:15 pm
Shoreham Hotel, Hampton Room

Critical Infrastructure Protection presents unique challenges for both the Federal Government and the private sector. DOT is working in new ways with the both the private sector and with civilian and law enforcement and intelligence agencies to help assure the continuity and integrity of the nation's critical infrastructures.

This new relationship must be focused on the sharing of sensitive vulnerability and threat information. Leading the Department's efforts is Admiral Jim Underwood, the Department's point of contact for CIP as our Sector Liaison Official.

Jim is now working closely with Mr. Ed Hamberger, President and CEO of the Association of American Railroads, who has taken on the challenge and responsibilities of the transportation Sector Coordinator, focusing initially on the issues affecting railroads.

Nancy Wilson will speak more on the AAR's perspective on this new relationship later in this session.

Y2K left us with an important lesson we must never forget, and must capitalize on B information systems now control practically every aspect of our lives. As some of you may have noticed, we even had a few residual Y2K glitches over this past New Year's weekend, just to remind us again.

Without computers, the National Airspace System would virtually shut down. Without computers, the nation's rail and transmission pipeline systems would slow to a crawl. Without Intelligent Transportation Systems, traffic lights would blink yellow, and emergency dispatch services, including 911, would cease to function.

The Washington Metro and other mass transit systems would either shut down, or default to total manual controls. UPS and FEDEX couldn't locate the Christmas presents you sent to Aunt Edith, or the critical spare part needed to restore a locomotive or an airplane to operation.

We must also use the lessons learned as we watch the growing pains of deregulation of electric power in the power grids in California. Compromise of the power grids, whether by overloading the system or by loss of computer control systems, has much greater and far reaching impacts than the loss of residential air conditioning on a hot California day.

Again, trains and planes will slow to a crawl, pipelines will shut down, traffic will snarl in metropolitan areas. Phone systems might be affected. And if they are, once again we lose the capability to communicate data from radar sites to the FAA to safely control aircraft, and dispatchers can't communicate with train engineers, pipeline control systems could be compromised.

As an example, we could shut down a major airport by losing the ability to operate landing systems. Y2K showed us the interdependencies of our critical systems are vast and largely unexplored.

We need to begin by protecting our own individual systems, then move ahead with getting a full understanding of the supporting infrastructures that keep the primary systems running.

Last year, the President's National Security Telecommunications Advisory Committee completed a two-year study on information-based risks to the nation's transportation information infrastructure. The study concluded: The transportation industry is increasingly reliant on IT and public networks;

I. Although a nationwide disruption of the transportation infrastructure is unlikely, even a local or regional disruption could have a significant impact;

II. Business pressures and widespread utilization of IT make large-scale, multimodal disruptions more likely in the future;

III. A need exists for a broad-base infrastructure assurance awareness program to assist all modes of transportation;

IV. The transportation industry could leverage ongoing research and development (R&D) initiatives to improve the security of the transportation information infrastructure;

V. Closer coordination is required between the transportation industry and other critical infrastructures.

Our joint DOT and industry CIP efforts will go a long way to address these issues, but we have a long way to go.

We are already cooperating with the Department of Defense, not only on strategic mobility, but also on critical infrastructure protection. Through Admiral Underwood's office, we've had great success to date working CIP issues with the United States Transportation Command and its agencies.

John Germanos from the Transportation Engineering Agency will speak more to that DOD-DOT cooperative relationship.

But we find ourselves, along with DOD and the transportation industry, in the uncomfortable situation of having a mandate to assess and mitigate our vulnerabilities, but with little funding to do so. Questions about FOIA and liability issues surrounding vulnerability assessments have slowed our moving ahead in a cooperative fashion with the transportation sector.

Without a clear funding mandate by the federal government to support these assessments and the subsequent corrective action that might be needed, DOT appropriately must assume a supporting role. We are and will continue to work cooperatively within the Federal government and with the industry to mitigate those vulnerabilities where we can, and most important, find ways to share information we all need to secure and assure our critical systems.

The Department is also expected not only to act as a partner in protecting the transportation infrastructure, but to protect our own critical infrastructure.

Dan Meehan will fill you in on our significant efforts to protect the Department's own critical infrastructure, particularly the National Airspace System. The FAA should be congratulated on recognizing the significance of protecting the Airspace System from intentional or accidental disruption, and focusing resources, as provided by the Congress, to that end. We must continue on the very highest priority with these efforts.

One of our biggest challenges is how to share information not only within the federal government, but also with FBI, the National Infrastructure Protection Center (NIPC), the transportation industry through our private sector coordinator, the Association of American Railroads (AAR), and various private sector Information Sharing and Analysis Centers serving key infrastructure sectors.

We must find a way to share what we learn with the owners and operators, without compromising national security or corporate sensitivities. We need to find a way to share information with the private sector that will be useful in protecting defense critical assets.

The world's greatest transportation system gives us the key network needed to drive the world's strongest economy. We must ensure this system of intermodal, interconnected roads and trucks, rails, air, pipelines, waterways, and mass transit is dependable, reliable, and available when we need it. The nation expects nothing less, and we must deliver.