United States Senate

COMMITTEE ON COMMERCE, SCIENCE,
AND TRANSPORTATION

WASHINGTON, DC 20510–6125

WEB SITE: http://commerce.senate.gov

July 14, 2009

The Honorable Ray LaHood
Secretary
U.S. Department of Transportation
1200 New Jersey Avenue, SE
Washington, DC 20590

Dear Secretary LaHood:

Earlier this year, I introduced comprehensive cybersecurity legislation (S. 773, the Cybersecurity Act of 2009) designed to improve the nation's overall cybersecurity posture and capabilities. I know that addressing cybersecurity is an ongoing management issue that requires constant vigilance.

On July 4, 2009, the U.S. Computer Emergency Readiness Team (US-CERT) received reports from several Federal agencies regarding a possible distributed denial-of-service attack against their web servers. This attack degraded the performance of the respective agencies' websites, which, in some cases, prevented legitimate users from accessing these important government resources. News reports indicate that this distributed denial-of-service attack was a widespread effort affecting numerous Federal departments and agencies, as well as several private sector sites, including the New York Stock Exchange and NASDAQ.

While I am aware that Federal systems are probed and attacked on a daily basis, I am alarmed by the magnitude of this incident and am deeply concerned about the Federal government's ability to respond to these attacks. In some cases, agency websites were down for a number of days—a condition that concerns me. Given the seriousness and breadth of this incident, I am requesting your assistance in understanding the cybersecurity preparedness of your department and effectiveness of its incident response capability. For example, I would like to learn:

- what plans or procedures the DOT has in place to respond to and mitigate cybersecurity incidents;
- how often the DOT tests and exercises its emergency recovery and continuity of operations plans;
- how often the DOT probes its own systems for vulnerabilities in order to take corrective action before they can be exploited; and
- whether contractor or service providers have specific cybersecurity-related service level agreements that provide assurance that attackers cannot use them as backdoor points of entry.

Finally, I am particularly concerned as to whether the DOT has the necessary resources (staff, expertise, or financial) to properly prepare for and effectively respond to major cybersecurity incidents.

Sincerely,

John D. Rockefeller, IV
Chairman
Senate Committee on
Commerce, Science, and Transportation