transportation systems, are owned and operated by private companies. If our critical infrastructures are targets, it is the private sector that is on the front line. To prevent and control attacks, the way to think differently about national security, as well as who is responsible for it. In the past, the defense of the Nation was about geography and an effective military command-and-control structure. However, attacks to these systems require an unprecedented exchange of information. It is essential to remove unnecessary barriers that prevent the private sector from sharing information. Because in many cases, releasing sensitive information into the public domain could have extremely negative consequences for business. CIISA requires the Director of the Office of Management and Budget to establish procedures for the Federal agencies to receive, acknowledge, mark, care, and store voluntarily submitted critical infrastructure information. Today, there is no uniform standard of care among Federal agencies.

CIISA requires that information and analyses from the Federal Government be shared back with the private sector in the form of notifications, warnings, and strategic analyses. The bill requires a Federal agency receiving voluntarily submitted critical infrastructure information to make reasonable efforts to do the following: one, analyze the information; two, determine the tactical and strategic implications for such information; three, identify interdependencies; and four, consider conducting further analysis in concert with other Federal agencies. Following this analysis, a Federal agency may issue warnings regarding potential threats to: one, individual companies; two, targeted industry sectors; three, the general public; or four, other government entities. Federal agencies must take appropriate actions to prevent the disclosure of the source of any voluntarily submitted critical infrastructure information that forms the basis for any warnings.

CIISA also requires the President to designate an entity within the executive branch to conduct strategic analyses of potential threats to critical infrastructure; and to submit reports and analyses to information sharing and analysis organizations and the private sector. These analyses draw upon this information submitted to the Federal Government by the private sector, as well as information from the Federal Government, such as national security and law enforcement information. The President is also required to submit a plan for developing strategic analysis capabilities in the Congress.

When competitors work closely to address common problems, antitrust concerns always surface. Security in a critical infrastructure is a national security issue. To encourage the private sector and Government each has different vantage points. It is my hope that this bill will help both entities work together to reduce the blind spot.

I thank Senator Kyl for his interest and leadership on this issue.

COMMENDING THE TRUCKING INDUSTRY

Mr. BROWNBACK. Madam President, I rise to speak today in recognition of the noble truck drivers across the Nation. For the past 2 weeks, our truckers have been valiant in their service to this country, delivering important supplies to the attack sites of New York City and Arlington, VA. Many of these truckers have been volunteering time, equipment, and use of their vehicles to supply these areas in efforts of relief.

For the past 2 weeks, our truckers have been valiant in their service to this country, delivering important supplies to the attack sites of New York City and Arlington, VA. Many of these truckers have been volunteering time, equipment, and use of their vehicles to supply these areas in efforts of relief.

The threats to our critical infrastructure are varied. Some of those threats are physical; some may come from cyberspace. From wherever they come, the private sector and Government must take appropriate actions to prevent the disclosure of the source of any voluntarily submitted critical infrastructure information that forms the basis for any warnings.

CIISA also requires the President to designate an entity within the executive branch to conduct strategic analyses of potential threats to critical infrastructure; and to submit reports and analyses to information sharing and analysis organizations and the private sector. These analyses draw upon this information submitted to the Federal Government by the private sector, as well as information from the Federal Government, such as national security and law enforcement information. The President is also required to submit a plan for developing strategic analysis capabilities in the Congress.

When competitors work closely to address common problems, antitrust concerns always surface. Security in a critical infrastructure is a national security issue. To encourage the private sector and Government each has different vantage points. It is my hope that this bill will help both entities work together to reduce the blind spot.

I thank Senator Kyl for his interest and leadership on this issue.

LOCAL LAW ENFORCEMENT ACT OF 2001

Mr. SMITH of Oregon. Madam President, I rise today to speak about hate crimes legislation I introduced with Senator KENNEDY in March of this year. The Local Law Enforcement Act of 2001 would add new categories to current hate crimes legislation sending a signal that violence of any kind is unacceptable in our society.

I would like to describe a terrible crime that occurred September 25, 1994 in Hollywood, CA. Three men and five juveniles wielding baseball bats and a golf club allegedly assaulted two gay