



**EDISON ELECTRIC
INSTITUTE**

December 21, 2001

The Honorable George W. Bush
President
The White House
1600 Pennsylvania Ave., NW
Washington, DC 20500

Dear Mr. President:

We are writing to express our strong support for two bills that address important cyber-security issues, H.R. 2435 (Davis-Moran) and S. 1456 (Bennett-Kyl). This support signals broad recognition by U.S. industry of the need to move from individual defense toward a common defense. Passage of these bills will constitute an important contribution to U.S. homeland security. With the clear support of your Administration, this legislation can be enacted.

Malicious computer attacks are now doubling in frequency every year. Threats are mutating rapidly. Historically, companies have treated their defenses as an individual corporate matter, but the increase in frequency, sophistication, and damage necessitates the sharing of very sensitive data. Simply put, industry and government need to get smarter and act more rapidly to ensure the nation's defense.

Our associations and companies have long supported critical infrastructure protection initiatives and likewise support the recent steps by your Administration to enhance those policies. Government law enforcement agencies seek detailed data about computer attacks for the purposes of better law enforcement, earlier detection, and the promotion of best practices in government and industry.

Today, however, corporate counsels advise their clients not to share voluntarily the details of computer attacks **with government agencies** because it could come back to haunt them. In their judgment, the risk that such data could ultimately be divulged through the Freedom of Information Act (FOIA) – even over the agency’s objections – is unacceptably high. We greatly appreciate your letter of September 26, 2001 to the National Security Telecommunications Advisory Committee (NSTAC) indicating your understanding of this situation and the corresponding statements by Administration officials.

The pending legislation (H.R. 2435, Davis-Moran, and S. 1456, Bennett-Kyl) corrects this situation by protecting the information from disclosure. The bills also provides limited use protection (not immunity) so that critical infrastructure information disclosed to the government cannot subsequently be used against the person submitting the information.

The legislation to alter the legal risk assessments necessarily carried out by corporate counsel also addresses concerns about sharing information **within industry**. The legislation includes a limited immunity for antitrust purposes for information shared solely for the purposes of facilitating the protection of critical infrastructures.. We accept the assurances from the Department of Justice that business review letters would be forthcoming for information sharing and analysis centers (ISACs) constituted under your Administration’s policies. Yet the issuance of even a set of such letters would prove inadequate, for at least three reasons. First, such ISACs would have to be constituted with a view toward satisfying the Department, as opposed to maximally fulfilling their primary mission. Second, there is the unavoidable negative implication for numerous other affected parties not in possession of a business review letter. Third, the ISACs are not the only organizations that have been constituted to share cyber threat information among industry sector members or with Federal agencies.

Beyond federal FOIA and antitrust, the proposed legislation goes on to clarify that computer attack data shared voluntarily with the government would not be disclosed either under the Federal Advisory Committee Act (FACA) or under state FOIA laws. We do recognize the federalism question which the second provision raises. At the same time, homeland defense is creating a need for federal, state, and local bodies to work jointly to a previously unprecedented degree. In some instances, first responders will not be from federal agencies. Information sharing ought not to dead-end at the federal level but should flow all the way down to the first responders. Without the same protection at the state level as at the federal, state agencies will face the same lack of revealing detail that federal agencies are experiencing today. The planning exercise for a possible terrorist strike at the Salt Lake City Olympics, “Black Ice,” exemplifies the desirability of a suite of targeted legal protections that bring in, rather than leave out, state and local authorities.

There has been, in our view, misunderstanding of the legislation by some critics. First, we are not calling into question the existing FOIA case law, which taken together suggests that a federal agency would win a test case. Rather, we are saying only that the risk of a loss of such a test case – as viewed by the parties bearing the risk – remains unacceptably high. More importantly, corporations should not be required to accept such risks, or the cost of litigation, when reporting significant cyber events in an attempt to protect the public interest. Second, this legislative package has only to do with disclosure of computer attack data and critical infrastructure protection. Normal regulatory information gathering will proceed unimpeded, as it should.

Mr. President, we applaud your bold leadership and urge you to act decisively with unequivocal support for confidence-building cyber disclosure legislation: a mutually reinforcing suite of targeted legal protections under federal antitrust and FACA statutes, as well as federal and state FOIA statutes. We seek your Administration's support in bringing such comprehensive legislation to the floors of the House and Senate as soon as possible.

Yours truly,

Tom Donohue
President
US Chamber of Commerce

Jerry Jasinowski
President
National Association of Manufacturers

Harris Miller
President
Information Technology
Association of America

Dave McCurdy
President
Internet Security Alliance

Steve Bartlett
President
Financial Services Round Table

Bruce J. Heiman
Executive Director
Americans for Computer Privacy

Robert Holleyman II
President and CEO
Business Software Alliance

Thomas Kuhn
President
Edison Electric Institute

CC: The Honorable Condoleezza Rice
The Honorable Tom Ridge
The Honorable Richard Clarke