

Submitting Organization: OMB Watch
Contact: Patrice McDermott
Paper name: E-Government and the Digital Divide
Category: Challenges and Opportunities | Digital Divide

Fight the online silence

BY Patrice McDermott
05/22/2000

"Government-enforced silence is more dangerous to our nation than thousands of unregulated voices."

It is not often that I find myself quoting the president of an industry association — in this case, John Haney, president of the Wisconsin Manufacturers Commerce association — in the name of public access and the right to know. But those words capture what is being proposed for government in the Cyber Security Information Act (H.R. 4246) and in a proposed rule implementing the 1999 Chemical Safety Information, Site Security and Fuels Regulatory Relief Act.

What the two rules have in common is government-enforced silence about public risks and vulnerabilities. And what they represent is the leading edge of a trend in limiting public access to government-held information.

The Chemical Safety Act required the Environmental Protection Agency to assess the benefits of giving the public access to Off-Site Consequence Analysis (OCA) information (which covers risks posed to the public from chemical accidents), and required the Justice Department to assess the increased risk of terrorist and other criminal activity from posting the information on the Internet. Justice and the EPA each proposed a rule that would prohibit the Internet posting of OCA information. Justice determined the posting of information could significantly increase the risk of terrorist or criminal activity.

And what reasons did Justice offer for the draconian measure of prohibiting meaningful public access to information specifically collected to protect the public? The chemical disaster at the Union Carbide plant in Bhopal, India — which Justice calls an "intentional release" despite consensus among government officials, community groups and even industry that it clearly was an accident — and press accounts of a group in Chechnya that planned an attack on a chemical facility.

Those examples are patently ridiculous, but they are still better than what is occurring in the area of critical infrastructure information, in which industry is crying out for government protection of information about risks and vulnerabilities in critical infrastructure.

In the Cyber Security Information bill, critical infrastructure is defined as "facilities or services whose disruption, incapacity or destruction" through things such as "misuse of, or by unauthorized means of, the Internet, public or private telecommunications systems" would have a debilitating impact on society.

What industry is asking the government for is effective silence about the risks to which the public is exposed.

Before we go any further down this path, government needs to engage in a public debate about which poses the greater risk to public health and safety: government-enforced silence, or people exercising their right to know about, and hold public actors accountable for, the risks and vulnerabilities to which government officials expose the American people.

– McDermott is an information policy analyst with OMB Watch, a government watchdog group in Washington, D.C.

Reproduced with permission of *Federal Computer Week*. Copyright May 22, 2000, FCW Government Technology Group. All rights reserved.