
The Competitive Enterprise Institute

1001 Connecticut Avenue NW • Suite 1250 • Washington, D.C. 20036 • (202) 331-1010 • <http://www.cei.org>

Committed to Advancing the Principles of Free Enterprise and Limited Government

May 21, 1999

No. 37

The Clean Air Act's Federal Terrorist Assistance Program

By Angela Logomasini¹

In recent years the United States has experienced the horrors of the terrorist attack of a federal building in Oklahoma City, the bombing of the World Trade Center, and even adolescent-led attacks in our public schools. Given widespread concern, federal lawmakers need to be keenly aware of any policy that could assist terrorist activity. One area of particular concern is a provision of the 1990 amendments to the federal Clean Air Act, which promises to produce a federal database that could assist terrorists in selecting potential targets. The database, which may end up on the Internet, could give terrorists access to the extent of damage they could produce and the number of lives they could take should they bomb a particular facility.

While some may say such claims are unfounded, the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), the International Association of Fire Chiefs and other security experts have expressed serious reservations about such a database, and they are pushing Congress for a solution.² Congress is looking into legislation, but at question is whether the final bill will solve the problem.

The problem arises under section 112(r) of the federal Clean Air Act. This provision mandates that certain industrial facilities prepare risk management plans (RMPs), which are supposed to help facilities and local communities reduce the risks of, and prepare for, potential accidental chemical releases. Each of the 66,000 regulated entities must submit a RMP to the EPA detailing measures they employ to prevent chemical releases and manage them when they occur. These plans, which entities must submit by June 21, must include an off-site-consequence analysis (OCA). The OCA details the potential impacts to the plant and the surrounding community (including such things as the number of fatalities and injuries) that would result under the "worst case scenario" from a catastrophic accidental chemical release. The law demands that the EPA make the information available to the public.

Unintended national security risks. The EPA initially proposed posting the information on the Internet, until FBI and other security experts raised concerns that the information would provide

¹ Angela Logomasini is Director of Risk and Environmental Policy at the Competitive Enterprise Institute.

² See, Statement of Robert M. Burnham, Chief, Domestic Terrorism (Federal Bureau of Investigation), before the Subcommittee on Clean Air, Wetlands, Private Property and Nuclear Safety of the Committee on Environment and Public Works, U.S. Senate, March 16, 1999. See also, statement of Chief John M. Eversole, International Association of Fire Chiefs, before the Subcommittee on Health & Environment and the Subcommittee on Oversight and Investigations of the House Commerce Committee, Feb. 10, 1999

terrorists with easy access to an anonymous, searchable database of potential targets and the potential fatality figures for such targets. At recent hearings, Robert E. Blitzer, former anti-terrorist expert for the FBI, explained the dire implications of putting the information on the Internet:

The plans [to post information on the Internet] would allow users to initiate Internet searches by facility name, area of the country, zip code, city, county, and state. A modified search by chemical type would allow a person using the EPA web site, to choose a portion of a city by zip code and tailor an attack by searching for certain chemicals. A search of this nature could be accomplished from anywhere in the world. Additionally, no record of such a query would be made. Further, searches could be tailored to developing information regarding chemical companies' mitigation and safeguarding capabilities.³

The EPA eventually backed down, but the Department of Justice soon explained in letter to Representative Tom Bliley that the EPA must release the information under Freedom of Information Act (FOIA) requests, and FOIA may even demand electronic and/or internet publication.⁴ To make matters worse, in December 7 report to the House Appropriations Committee, the FBI notes that environmental activists warned the EPA that they would access the information under the FOIA and post it on the Internet themselves if necessary.⁵

Activists ignore public health and safety. Ignoring just about every security expert in the business, environmental groups contend they know better. In recent congressional testimony, Thomas Nathan of the National Environmental Trust admitted that, "making the public aware of chemical use risks over the Internet would amplify this inherent, pre-existing risk."⁶ He justifies amplifying the risk on the grounds that "the risks emanate from the toxic chemical use," not Internet publication of data. The supposed answer is to reduce, and eventually eliminate, such chemicals. But this agenda does not take into account that the chemicals environmentalists call "toxic" produce life-saving pharmaceuticals as well as the hiking equipment environmentalists use and the chlorine that keeps at the public pools clean and safe for children, among many other items that improve our quality of life. We can either promote policies that allow firms to manage these risks, or we trade off all these quality of life benefits.

Consider environmentalists' faulty logic by applying the following analogy: Flying on airplanes poses some small threat of an accident. Because the risk of airplane accidents is inherent to flying, traveling by airplane is the problem under this "logic." Therefore, the government should force airlines to report all their vulnerabilities and outline all the ways that accidents could occur, in the process revealing all the potential ways that terrorists could undermine airplane safety. Under these circumstances, it's okay to increase terrorist risks because then public would then know the real source

³ Statement of Robert E. Blitzer, former Section Chief, Domestic Terrorism/Counter Terrorism Planning Section, Federal Bureau of Investigation, Before the Subcommittee on Clean Air, Wetlands, Private Property and Nuclear Safety of the Committee on Environment and Public Works, U.S. Senate, March 16, 1999.

⁴ "EPA Cannot Refuse FOIA Requests for Worst-Case-Scenario Data, DOJ Says," *Pesticide & Toxic Chemical News*, April 22, 1999.

⁵ "House Commerce Committee to Review Superfund and Worst-Case Legislation," *Chemical Market Reporter*, January 4, 1999.

⁶ Testimony of Thomas Nathan, Research Director, National Environmental Trust, before the Subcommittee on Clean Air, Wetlands, Private Property and Nuclear Safety of the Committee on Environment and Public Works, U.S. Senate, March 16, 1999.

of the risks: flying on airplanes. Eventually, such public “education” will eliminate the security risk of flying (by putting an end to the airline industry).

Only safe answer is limited and controlled access to sensitive data. Security specialists have suggested amending FOIA and the Clean Air Act to produce a closed system whereby the federal government would only provide this information to local emergency planners. This solution is only one that will adequately ensure that this information is not used to assist terrorists.

Keeping information secure and local has worked in New Jersey, according to Ben Laganga, Emergency Management Coordinator for the densely populated and industry-intensive Union County, New Jersey. In New Jersey, worst case scenario information is already available under state law, but only to emergency planners or by closely monitored requests. According to Laganga, it is better “to monitor those individuals who are requesting the information. If the information is available on the Internet, there is no way to know who is accessing that information, and quite frankly, how they are using it.” If the federal government makes the information available for others to put online it “could lead to an increase in terrorist acts in our state and throughout the county,”⁷ noted Laganga to a Senate committee.

In addition, there are better ways to communicate risks to communities at the local level than to produce federal databases of sensitive information. For instance, local officials can facilitate information exchange. In fact, according to a survey recently completed by the Competitive Enterprise Institute and *the polling company*, Americans prefer to access this information from local and state sources (65 percent), and few (8 percent) trust the federal government to provide such information.⁸ The public’s preference for local information sharing is not surprising. More constructive information comes from local exchanges between facilities and community organizations and emergency planners than from heavy-handed federal programs. Such voluntary exchanges already exist. Through this process, facilities hear concerns from the community and gain community trust through information exchange via public meetings, plant tours, and the like.

Pending Bills Make One Critical Change, but Serious Problems Remain

To address the problems with the current law, the Senate Environment and Public Works Committee recently approved a bill, S. 880, which largely incorporates recommendations made by the Administration. In the House, Commerce Committee chairman Tom Bliley (R-VA) has proposed similar legislation (H.R. 1790).

Both the Senate and House bills would make one critical improvement to existing law. They would exempt OCA data from Freedom of Information Act (FOIA) requests. As a result, the EPA won’t have to provide full or electronic copies of the all the OCA under the Freedom of Information Act requirements.

⁷ Testimony of Ben Laganga, Union County, New Jersey Emergency Management Coordinator, Subcommittee on Clean Air Wetlands, Private Property and Nuclear Safety, Committee on Environment and Public Works, U.S. Senate, March 16, 1999.

⁸ *National Environmental Survey*, prepared by *the polling company* for the Competitive Enterprise Institute, January 1999.

Bills guarantee Internet publication, make EPA chief security officer. However, the benefits of the FOIA exemption are largely negated because neither bill eliminates Clean Air Act mandates that the EPA make this information public. To the contrary, both bills mandate that agency officials provide paper copies when an individual requests OCAs. The EPA may provide copies of all OCAs, or it may limit individual requesters to information on a specified number of facilities. But even if EPA employs limits, environmental activists can employ numerous individuals to access all companies' information to assemble the complete database.

To meet Clean Air Act mandates, both bills also give EPA bureaucrats – rather than qualified security experts or security agencies – broad authority to issue rules on how to release data and in what format. When setting rules, the bill states that the EPA “shall consult” with “appropriate Federal Agencies,” but that is the extent of their limitations. Nothing bars EPA bureaucrats from ignoring the advice of security experts.

The Pending Bills Also Pose Other Serious Problems

Local repositories are window dressing given other mechanisms for disclosure. Both bills also demand that the EPA ensure that electronic or paper copies of all risk management plans relevant to an area be available at local public repository (such as a library), for viewing but not copying. If this local information is available, why have EPA provide paper copies? Local access is supposed to be an *alternative* to EPA distribution, rather than an additional method of distribution.

The bill would protect the identity of potential terrorists. Both bills bar the EPA bureaucrats and state officials from keeping records on those who request information unless the president, Congress, or state legislatures pass laws demanding such record keeping. It is curious that the only limitation on the EPA is related to keeping track of the names of potential terrorists and those who will publish the information online.

Both bills wrongly shift the blame. Another provision in both bills would require the Attorney General to review industry security practices and recommend to Congress ways to make plants safer – as if this government-created problem was caused by faulty industry security practices. The provision will likely lead to future “environmental” regulation that will be based on the faulty assumption that EPA bureaucrats know how to promote security better than local security officials, emergency planners, and those who operate facilities in the private sector.

Conclusion. Public security should be the number one goal when reforming section 112(r) of the Clean Air Act. Both bills will prevent FOIA requests on sensitive OCA data and may enable the EPA to delay Internet publication. However, neither will prevent Internet publication because they both provide paper copies that will enable others to post the information on line. The way to secure this information would be to provide it only to those who need it for risk management: local emergency planners.