CEI OnPoint

Competitive Enterprise Institute
1001 Connecticut Ave NW • Suite 1250 • Washington, DC 20036
202.331.1010 • www.cei.org

Advancing Liberty – From the Economy to Ecology

June 28, 2007 **No. 117**

The Flexibility Solution:

How Private Enterprise can Improve Infrastructure Security

By Eli Lehrer and Wayne Crews*

America has not done enough to protect the networks of roads, train lines, pipelines, power wires, ports, and fiber-optic networks that constitute the nation's critical infrastructure. This infrastructure, indeed, faces threats from all directions, from nuisances to existential risks. The September 11, 2001 terrorist attacks and Hurricane Katrina showed the vulnerability of our systems. A snow storm can clog highways for weeks. A tornado can shut down power for millions. A malicious virus could cripple the Internet. Another airplane hijacking could paralyze long distance travel. A nuclear terrorist attack could destroy much in a major city and send the entire economy into a tailspin. While we can always mitigate—and in the case of terrorist attacks, prevent—these events, neither the government nor private enterprise can provide total safety. We can, however, make one perfectly safe prediction: The United States will continue to face threats to our critical infrastructure. The nation must protect itself.

Over the last decade, government has taken an ever-growing role in providing this protection. Of course, government has a role to play in defending the country from threats both natural and man-made. But we will hurt our own security by allowing government's role to grow too large. In this paper, we outline a new approach for protecting the nation, one that allows for the best use of both government and private efforts. We provide examples of how we might apply that framework to the Internet, to our air travel system, and to the nation's power grid. Good security against most threats requires flexibility, and private enterprise, on balance, provides greater flexibility than does government.

Limits to Government's Role. Countries create governments mainly to protect society against threats, foreign and domestic. The government deploys the military, takes on the primary function of policing, runs the courts, and enforces contracts. Yet individuals often still need private security guards, privately built flood walls, privately

* *Eli Lehrer is a Senior Fellow at the Competitive Enterprise Institute (CEI). Wayne Crews is Vice President for Policy and Director of Technology Studies at CEI.*

run power-grid safety controls, door locks, barbed wire, firewalls, and anti-virus software. People could not expect a reasonable level of safety in a nation without government, nor could they expect safety in a society in which private actors did nothing to provide security.

Because it has the power to levy taxes, seize private property, and use force, government can almost always marshal more resources than any private entity. It's almost always easier—although not necessarily better—for government to build critical infrastructure. Government entities have taken on responsibilities for maintaining nearly all roads, some rail lines, and a significant portion of the Internet. But government faces two enormous disadvantages. First, it's inflexible, and therefore tends toward one-size-fits-all solutions. Second, in a democracy people will often express grievance when they believe that government has allocated resources to their disadvantage. In many security situations, these two disadvantages can add up to disaster: Government cannot respond to ever-changing threats from non-state terrorist actors, and it responds to natural disasters quite slowly. When government wants to change or extend what it does, it needs political approval. Private enterprise does not.

Government Rigidity vs. Private Flexibility. The private sector has a harder time marshaling resources than does the government but it is not saddled with these disadvantages. Private firms can innovate much more quickly than can government—even try fundamentally different approaches to existing problems.

Individuals already enjoy an almost entirely private system to secure personal Internet access. Private security also protects the efficacy of the fiber optic cables that prove a key part of our infrastructure. This success arose out of government failure. Congress has passed laws—such as the 2003 CAN SPAM Act—to criminalize certain online behaviors and malicious computer programs.[1] But the nature of the Internet has made it virtually impossible to enforce such bans.

Thus, the need for security software has intensified. Early efforts—both public and private—focused on identifying particular sequences of known malicious code and blocking them. This approach has some merit and still finds some use, but it has a fatal flaw: It is inflexible and, thus unable to protect the decentralized Internet. Thus, the market has found a solution. Newer technologies—including built-in measures in both the Macintosh OS X Panther and Windows Vista operating systems—give individuals the power to refuse "admission" to any computer or individual that wants to access data on a system.[2] Individuals get prompted if a person or computer program tries to access data, rewrite a hard disk, or redirect a Web browser. If a particular security solution proves particularly difficult, then users can switch operating systems or add additional software.[3]

New Strategies for Airline Security. We should consider how to apply similar approaches to airline security. As it exists, the system remains terribly rigid and, perhaps, dangerously ineffective. According to Robert Poole of the Reason Public Policy Institute, the federal government's "knee-jerk response" of taking over passenger screening in the wake of 9/11, by focusing so heavily on passenger screening, misses the possibly risky

access to sensitive areas retained by caterers, refuelers, cleaning staff, and other support personnel. Moreover, staffing security functions with civil servants severely diminishes flexibility in hiring.[4]

Government regulation of the industry itself creates other problems. In his book *Beyond Fear: Thinking Sensibly About Security In an Uncertain World*, security expert Bruce Schneier writes, "[O]nly two effective antiterrorism countermeasures were taken in the wake of 9/11: strengthening the cockpit doors and passengers learning they need to fight back. Everything else—let me repeat that: *everything else*—was only minimally effective, at best.[5] Prior to 9/11, economist William L. Anderson points out that government regulation stopped this reform. "While it makes for good press for attorneys and judges, the idea that Boeing on its own could have ordered 'secure' cockpit doors is a laugher," he notes. "Any unilateral attempt by any aircraft maker to act without FAA direction is always met with swift action against the manufacturer."[6]

In addition to deregulating some aspects of aircraft construction, other non-governmental options might include private airline ID cards and prescreening of passengers (something the federal law allows but has yet to happen), better employee background checks, and even pilot biometrics that would allow planes to only be flown with a live, identified pilot in the seat. This would prevent any plane being used as a guided missile. We cannot know exactly which threats are the most realistic, but we can expect terrorists to keep on looking for weaknesses to exploit. By relying so heavily on government, we have closed off many avenues for private innovation.

Naturally, some of the steps the government has taken probably *have* resulted in marginal safety improvements. But the government's narrow focus on passenger and luggage screening leaves a lot of holes in the system for terrorists to exploit. For the most part, security procedures are exactly the same at every airport in the country. If the federal government makes even one serious mistake, it's possible that security could fail at every airport. If terrorists find such a hole, they could carry out a massive attack. Thus, the government might take a page from successful personal cybersecurity efforts and make private companies accountable for access to all airport—and for that matter, seaport—facilities. Government could play a role in verifying the quality of security personnel and test out the systems but, on balance, private firms could probably do a better job than the government in filling any holes that might emerge.

Where it has been allowed to function, the market has found ways to deal with problems of the existing system. One New-York based airline specializing in transatlantic travel, for example, has hired its own screeners to speed its passengers through security.[7]

Electrical Grid Security. Similarly, we should look for ways to increase the flexibility of measures to protect the nation's electrical infrastructure. In electricity, for example, mandates to supposedly enhance "reliability" can actually impair operation of the grid. The Northeastern blackout of August 2003 bolstered calls for implementing central power grid management via "independent system operators."[8] While such moves might prevent blackouts, they would might not improve the overall security or stability of the

system. A system with a single "independent system operator" can go down entirely if the "independent operator" comes under attack or experiences a serious glitch. Even if each of its nodes proves *less* secure than a single central command center, a decentralized system would be more robust, since damage in one part of the system would be more easily contained.

Similarly, a one-size-fits-all approach to atomic security could lead to the creation of dangerous holes in all of the nation's nuclear plants that terrorists could exploit. Finally, efforts to centralize electrical power control entirely ignore real and potential technologies that could improve the efficacy of the power grid and thus its security. Electrical power companies already have everything to lose and nothing to gain when the lights to go out.

Massive centralization, furthermore, can "socialize" critical infrastructure to such a degree that genuine deregulation simply cannot occur. Thus, government's self-appointed role in managing major components of the nation's infrastructure and security cannot be properly scaled back when and if the market comes up with a better solution.[9] The best system would avoid over-centralization and let private energy companies decide how they can secure their own infrastructure, keep the lights on, and protect their investments.

Conclusion. Government has an important role to play in securing critical infrastructure. Only government can protect against many serious attacks and only government can make the laws that bring attackers to justice. But government, in the end, lacks the flexibility that is key to confronting many new threats as they emerge. In more cases than not, private security will work better than anything government can muster.

Notes

[1] For more on the particulars of these government efforts see: Federal Trade Commission. "The CAN SPAM ACT: Requirements for Business," January 23, 2004, http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.htm.

[2] The seminal work on Capability based security is Levy, Henry M., *Capability-Based Computer Systems*, Digital Equipment Corporation 1984.

[3] Krebs, Brian. "Windows Security Flaw is 'Severe." *Washington Post,* December 30, 2005, p. D01, http://www.washingtonpost.com/wp-dyn/content/article/2005/12/29/AR2005122901456.html.

[4] Robert W. Poole Jr., "Learn From Experience On Airport Security," *Heritage Foundation Backgrounder*, No. 1493, October 15, 2001. http://www.heritage.org/Research/NationalSecurity/BG1493.cfm.

[5] Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security In an Uncertain World*, Copernicus Books: New York, 2003. pp. 247-8.

[6] William L. Anderson, "Who is to Blame for 9-11?" Mises Institute. December 4, 2003, http://www.mises.org/fullstory.asp?control=1387.

[7]The airline is EOS Airlines, For information on its policies see: "Security Policies," http://www.eosairlines.com/flyeos/overview/home.jsf;jsessionid=8AFF3ED549363317E57FEBBC68DD6F77.

[8] For an overview of typical regulatory reactions to the blackouts, see Peter Behr, "Legislation Would Set Rules for Grid," *Washington Post*, November 15, 2003. p. A01, http://www.washingtonpost.com/ac2/wp-dyn/A42844-2003Nov14?language=printer.

[9] For example see Eric Pianin and Bill Miller, "Businesses Draw Line on Security," *Washington Post*, September 5, 2002, p. A1, http://www.washingtonpost.com/ac2/wp-dyn/A38213-2002Sep4?language=printer.