

Statement

“Critical Infrastructure: Who’s In Charge?”
Senator Joseph Lieberman
Chair, Committee on Governmental Affairs Committee
Thursday, October 4, 2001
Statement for the Record

Today, the Governmental Affairs Committee holds another in its continuing series of hearings into the security of our nation’s critical infrastructure, and the vulnerability of our homeland to enemy attack.

Since the attack on America that occurred September 11, we have embarked on a fundamental re-evaluation of how best to protect our nation, not only at its borders, but also within its core infrastructure. Critical infrastructure has been described as our nation’s skeleton, but it is more aptly our nation’s vital organs. The critical infrastructure - our financial, transportation and communications networks, our utilities, public health system, law enforcement and emergency services - is what keeps the country humming, what enables us to interact, live good lives with one another, what, in fact, makes America work.

The morning after September 11, we held a hearing on these matters, which served as a general introduction to critical infrastructure. The hearing had been previously scheduled and was focused on cyber security. On September 21, we held a hearing on the broader question of whether government is organized to respond to the challenge of homeland threats. And on the 25th, we narrowed our sights to look at airline security, and passenger screening in particular.

Today, the Committee delves again into issues of critical infrastructure, to determine who’s really responsible for protecting and ensuring our infrastructure’s security, both in the public and the private realms.

To do this requires a review of Presidential Decision Directive (PDD) 63, signed by President Clinton in 1998, which established the current framework for protecting our nation’s critical infrastructure. The directive asked agencies to develop and implement plans that would protect government-operated infrastructures, and it called for a dialogue between government and the private sector to develop a national plan by the year 2003.

PDD-63 - as it is known bureaucratically - identified the following eight categories of critical infrastructure that need protection. They are: information and communications; banking and finance; water supply; transportation, including aviation, highways, mass transit, pipelines, rail, and waterborne commerce; emergency and law enforcement services; emergency fire and continuity of government services; public health services; and electric power, oil and gas production and storage. The directive required each federal agency to secure its own critical infrastructure and to identify a chief officer to assume that responsibility.

The directive also established several new offices to oversee and coordinate critical infrastructure protection. One was a National Coordinator designated to ensure that a national plan was developed. The coordinator

would be supported by a Critical Infrastructure Assurance Office (CIAO), to be located within the Export Administration of the Department of Commerce.

The directive created a joint FBI and private sector office - the National Infrastructure Protection Center (NIPC), which serves as the focal point for federal threat assessment, vulnerability analysis, early warning capability, law enforcement investigations, and response coordination. NIPC is also the private sector point of contact for information sharing.

Finally, the directive recommended that we have the capability to detect and respond to cyber attacks while they are in progress. The Federal Computer Incident Response Center (FedCIRC) gives agencies the tools to detect and respond to such attacks, and it coordinates response and detection information.

The Committee is fortunate to hear from distinguished representatives from each of these offices – John Tritak, director of the Critical Infrastructure Assurance Office, Ronald Dick, director of the National Infrastructure Protection Center, and Sally McDonald, director of the Federal Computer Incident Response Center - about the government’s successes and failures in implementing PDD-63, and what we must still do to safeguard our critical infrastructure. They will help us assess government’s response to protecting our infrastructure, in part by answering the question that this hearing’s title poses: “Who’s in charge?” What offices are responsible for the different aspects of maintaining our critical infrastructure protection? And ultimately, is our system the most comprehensive and effective that it can be in responding to threats?

The Presidential Decision Directive was a significant first step in our efforts to safeguard our critical infrastructure, but it was just that – a first step. Other measures must be taken to build upon the work the directive initiated. We must also realize that the challenge is complicated because a mix of public and private entities controls so many elements of our critical infrastructure. Presidential Directive-63 envisaged a partnership role for the private sector when it proposed the creation of a private sector Information Sharing and Analysis Center (ISAC). The hope was that sharing information – including threats, vulnerabilities, incidents, and responses – would occur between the NIPC and the individual sector-level Information Centers.

The Committee is privileged to hear from four representatives of the private sector today to testify about the efforts that have been made in the private sector, and to get their views on what more can and should be done to protect infrastructure, as well as who should bear the responsibility for those initiatives. The Committee will hear from Frank Cilluffo, of the Center for Strategic and International Studies, Joseph Nacchio, CEO of Qwest Communications, and Jamie Gorelick, Vice Chair of Fannie Mae. Finally, Kenneth Watson, president of the Partnership for Critical Infrastructure Protection Security, will describe how private sector industries are communicating with each other and conveying critical information to the government.

With the efficient partnership of both the public and private spheres, we will strengthen our defenses against the types of insidious acts that all of us are now only too painfully aware of. I look forward to this committee continuing its own bipartisan partnership in considering the questions of “who’s responsible” for our critical infrastructure, and as appropriate, making recommendations to our colleagues in Congress.

Thank you.