What Are Critical Infrastructures?

Critical Infrastructures are those industries identified in Presidential Decision Directive—63 and version 1.0 of the National Plan for Information Systems Protection, deemed vital for the continuing functioning of the essential services of the United States. These include telecommunications, information technology, financial services, oil, water, gas, electric energy, health services, transportation, and emergency services.

What Is the Problem?

90% of the nation’s critical infrastructures are owned and/or operated by the private sector. These industries are inter-connected through networks. This has made them more efficient, but it has also increased the vulnerability of multiple sectors of the economy to attacks on particular infrastructures. According to the Carnegie-Mellon Computer Emergency Response Team (CERT), cyber attacks on critical infrastructures have increased exponentially over the past three years. This trend is expected to continue for the foreseeable future. In our free market system, it is not feasible to have a centralized-government monitoring function. A voluntary national industry-government information sharing system is needed in order for the nation to create an effective early warning system, find and fix vulnerabilities, benchmark best practices and create new safety technologies.

How Do Industries and the Government Share Information?

Based on PDD–63 and the National Plan, a number of organizations have been created to foster industry-government cooperation. These include Information Sharing and Analysis Centers (ISACs). ISACs are industry-specific and have been set up in every financial services, telecommunications, IT, and electric energy industries. Others are in the process of being organized. ISACs vary in their membership structures and relationship to the government. Most of them have a formal government sector liaison as their principal point of contact.

What Are Current Concerns?

Companies are concerned that information voluntarily shared with the government that reports on or concerns corporate security may be subject to FOIA. They are also concerned that lead agencies may not be able to effectively control the use or dissemination of sensitive information because of similar legal requirements. Access to sensitive information may fall into the hands of terrorists, criminals, and other individuals and organizations capable of exploiting vulnerabilities and harming the U.S. Unfiltered, unmediated information may be misinterpreted by the public and undermine public confidence in the country’s critical infrastructures. Also, competitors and others may use that information to the detriment of a reporting company, or as the basis for litigation. Any and all of these possibilities are reasons why the current flow of voluntary data is minimal.

What Can Be Done?

Possible solutions include creating an additional exemption to current FOIA laws. There are currently over 80 specific FOIA exemptions throughout the body of U.S. law, so it is clear that other voluntarily shared information that could affect national security is consistent with the intent and application of FOIA. Another solution is to build on existing relevant legal precedents such as the 1998 Y2K Information and Readiness Disclosure Act, the 1984 National Cooperative Research Act, territorially limited court rulings, and individual, advisory Department of Justice Findings.

Why Pursue a Legislative Solution?

The goal is to provide incentives for voluntary information sharing. Legislation can add legal clarity that will provide one such incentive, as well as demonstrate the support and commitment of Congress to increasing critical infrastructure assurance.

PERSONAL EXPLANATION

HON. SHELLEY BERKLEY
OF NEVADA
IN THE HOUSE OF REPRESENTATIVES
Tuesday, July 10, 2001

Ms. BERKLEY. Mr. Speaker, flight delays caused me to miss rollcall votes Nos. 186, 187, and 188. Had I been present, I would have voted “yes” on No. 186, “yes” on No. 187, and “yes” on No. 188.