

Presidential Decision Directive 63    PROTECTING AMERICA'S CRITICAL INFRASTRUCTURE

This Presidential Directive builds on the recommendations of the President's Commission on Critical Infrastructure Protection. In October 1997, the Commission issued its report calling for a national effort to assure the security of the United States' increasingly vulnerable and interconnected infrastructures, such as telecommunications, banking and finance, energy, transportation, and essential government services.

Presidential Decision Directive 63 is the culmination of an intense, interagency effort to evaluate those recommendations and produce a workable and innovative framework for critical infrastructure protection. The President's policy:

Sets a goal of a reliable, interconnected, and secure information system infrastructure by the year 2003, and significantly increased security to government systems by the year 2000, by:

    Immediately establishing a national center to warn of and respond to attacks.

    Ensuring the capability to protect critical infrastructures from intentional acts by 2003.

Addresses the cyber and physical infrastructure vulnerabilities of the Federal government by requiring each department and agency to work to reduce its exposure to new threats;

Requires the Federal government to serve as a model to the rest of the country for how infrastructure protection is to be attained;

Seeks the voluntary participation of private industry to meet common goals for protecting our critical systems through public-private partnerships;

Protects privacy rights and seeks to utilize market forces. It is meant to strengthen and protect the nation's economic power, not to stifle it.

Seeks full participation and input from the Congress.

PDD-63 sets up a new structure to deal with this important challenge:

    a National Coordinator whose scope will include not only critical infrastructure but also foreign terrorism and threats of domestic mass destruction (including biological weapons) because attacks on the US may not come labeled in neat jurisdictional boxes;

    The National Infrastructure Protection Center (NIPC) at the FBI which will fuse representatives from FBI, DOD, USSS, Energy, Transportation, the Intelligence Community, and the private sector in an unprecedented attempt at information sharing among agencies in collaboration with the private sector. The NIPC will also provide the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks,

investigating threats and monitoring reconstitution efforts;

Information Sharing and Analysis Centers (ISACs) are encouraged to be set up by the private sector in cooperation with the Federal government and modeled on the Centers for Disease Control and Prevention;

A National Infrastructure Assurance Council drawn from private sector leaders and state/local officials to provide guidance to the policy formulation of a National Plan;

The Critical Infrastructure Assurance Office will provide support to the National Coordinator's work with government agencies and the private sector in developing a national plan. The office will also help coordinate a national education and awareness program, and legislative and public affairs.