**SEC. 1015. EXPANSION AND REAUTHORIZATION OF THE CRIME IDENTIFICATION TECHNOLOGY ACT FOR ANTITERRORISM GRANTS TO STATES AND LOCALITIES.**

Section 102 of the Crime Identification Technology Act of 1998 (42 U.S.C. 14601) is amended—

(1) in subsection (b)—

(A) in paragraph (16), by striking ''and'' at the end;

(B) in paragraph (17), by striking the period and inserting ''; and''; and

(C) by adding at the end the following:

''(18) notwithstanding subsection (c), antiterrorism purposes as they relate to any other uses under this section or for other antiterrorism programs.''; and

(2) in subsection (e)(1), by striking ''this section'' and all that follows and inserting ''this section $250,000,000 for each of fiscal years 2002 through 2007.''.

**SEC. 1016. CRITICAL INFRASTRUCTURES PROTECTION.**

(a) SHORT TITLE.—This section may be cited as the ''Critical Infrastructures Protection Act of 2001''.

(b) FINDINGS.—Congress makes the following findings:

(1) The information revolution has transformed the conduct of business and the operations of government as well as the infrastructure relied upon for the defense and national security of the United States.

(2) Private business, government, and the national security apparatus increasingly depend on an interdependent network of critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors.

(3) A continuous national effort is required to ensure the reliable provision of cyber and physical infrastructure services critical to maintaining the national defense, continuity of government, economic prosperity, and quality of life in the United States.

(4) This national effort requires extensive modeling and analytic capabilities for purposes of evaluating appropriate mechanisms to ensure the stability of these complex and interdependent systems, and to underpin policy recommendations, so as to achieve the continuous viability and adequate protection of the critical infrastructure of the Nation.

(c) POLICY OF THE UNITED STATES.—It is the policy of the United States—

(1) that any physical or virtual disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States;

(2) that actions necessary to achieve the policy stated in paragraph (1) be carried out in a public-private partnership involving corporate and non-governmental organizations; and

(3) to have in place a comprehensive and effective program to ensure the continuity of essential Federal Government functions under all circumstances.

(d) ESTABLISHMENT OF NATIONAL COMPETENCE FOR CRITICAL INFRASTRUCTURE PROTECTION.—

(1) SUPPORT OF CRITICAL INFRASTRUCTURE PROTECTION AND CONTINUITY BY NATIONAL INFRASTRUCTURE SIMULATION AND ANALYSIS CENTER.—There shall be established the National Infrastructure Simulation and Analysis Center (NISAC) to serve as a source of national competence to address critical infrastructure protection and continuity through support for activities related to

counterterrorism, threat assessment, and risk mitigation.

(2) PARTICULAR SUPPORT.—The support provided under paragraph (1) shall include the following:

(A) Modeling, simulation, and analysis of the systems comprising critical infrastructures, including cyber infrastructure, telecommunications infrastructure, and physical infrastructure, in order to enhance understanding of the large-scale complexity of such systems and to facilitate modification of such systems to mitigate the threats to such systems and to critical infrastructures generally.

(B) Acquisition from State and local governments and the private sector of data necessary to create and maintain models of such systems and of critical infrastructures generally.

(C) Utilization of modeling, simulation, and analysis under subparagraph (A) to provide education and training to policymakers on matters relating to—

(i) the analysis conducted under that subparagraph;

(ii) the implications of unintended or unintentional disturbances to critical infrastructures; and

(iii) responses to incidents or crises involving critical infrastructures, including the continuity of government and private sector activities through and after such incidents or crises.

(D) Utilization of modeling, simulation, and analysis under subparagraph (A) to provide recommendations to policymakers, and to departments and agencies of the Federal Government and private sector persons and entities upon request, regarding means of enhancing the stability of, and preserving, critical infrastructures.

(3) RECIPIENT OF CERTAIN SUPPORT.—Modeling, simulation, and analysis provided under this subsection shall be provided, in particular, to relevant Federal, State, and local entities responsible for critical infrastructure protection and policy.

(e) CRITICAL INFRASTRUCTURE DEFINED.—In this section, the term ''critical infrastructure'' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such

systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

(f) AUTHORIZATION OF APPROPRIATIONS.—There is hereby authorized for the Department of Defense for fiscal year 2002, $20,000,000 for the Defense Threat Reduction Agency for activities of the National Infrastructure Simulation and Analysis Center under this section in that fiscal year.

Passed the House of Representatives October 24, 2001.

Attest: JEFF TRANDAHL,

*Clerk.*