

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

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

7 (1) in subsection (b)—

8 (A) in paragraph (16), by striking “and”
9 at the end;

10 (B) in paragraph (17), by striking the pe-
11 riod and inserting “; and”; and

12 (C) by adding at the end the following:

13 “(18) notwithstanding subsection (c),
14 antiterrorism purposes as they relate to any other
15 uses under this section or for other antiterrorism
16 programs.”; and

17 (2) in subsection (e)(1), by striking “this sec-
18 tion” and all that follows and inserting “this section
19 \$250,000,000 for each of fiscal years 2002 through
20 2007.”.

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

22 (a) **SHORT TITLE.**—This section may be cited as the
23 “Critical Infrastructures Protection Act of 2001”.

24 (b) **FINDINGS.**—Congress makes the following find-
25 ings:

1 (1) The information revolution has transformed
2 the conduct of business and the operations of gov-
3 ernment as well as the infrastructure relied upon for
4 the defense and national security of the United
5 States.

6 (2) Private business, government, and the na-
7 tional security apparatus increasingly depend on an
8 interdependent network of critical physical and in-
9 formation infrastructures, including telecommuni-
10 cations, energy, financial services, water, and trans-
11 portation sectors.

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

17 (4) This national effort requires extensive mod-
18 eling and analytic capabilities for purposes of evalu-
19 ating appropriate mechanisms to ensure the stability
20 of these complex and interdependent systems, and to
21 underpin policy recommendations, so as to achieve
22 the continuous viability and adequate protection of
23 the critical infrastructure of the Nation.

24 (c) POLICY OF THE UNITED STATES.—It is the pol-
25 icy of the United States—

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

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

11 (3) to have in place a comprehensive and effec-
12 tive program to ensure the continuity of essential
13 Federal Government functions under all cir-
14 cumstances.

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

17 (1) SUPPORT OF CRITICAL INFRASTRUCTURE
18 PROTECTION AND CONTINUITY BY NATIONAL INFRA-
19 STRUCTURE SIMULATION AND ANALYSIS CENTER.—

20 There shall be established the National Infrastruc-
21 ture Simulation and Analysis Center (NISAC) to
22 serve as a source of national competence to address
23 critical infrastructure protection and continuity
24 through support for activities related to

1 counterterrorism, threat assessment, and risk miti-
2 gation.

3 (2) PARTICULAR SUPPORT.—The support pro-
4 vided under paragraph (1) shall include the fol-
5 lowing:

6 (A) Modeling, simulation, and analysis of
7 the systems comprising critical infrastructures,
8 including cyber infrastructure, telecommuni-
9 cations infrastructure, and physical infrastruc-
10 ture, in order to enhance understanding of the
11 large-scale complexity of such systems and to
12 facilitate modification of such systems to miti-
13 gate the threats to such systems and to critical
14 infrastructures generally.

15 (B) Acquisition from State and local gov-
16 ernments and the private sector of data nec-
17 essary to create and maintain models of such
18 systems and of critical infrastructures gen-
19 erally.

20 (C) Utilization of modeling, simulation,
21 and analysis under subparagraph (A) to provide
22 education and training to policymakers on mat-
23 ters relating to—

24 (i) the analysis conducted under that
25 subparagraph;

1 (ii) the implications of unintended or
2 unintentional disturbances to critical infra-
3 structures; and

4 (iii) responses to incidents or crises
5 involving critical infrastructures, including
6 the continuity of government and private
7 sector activities through and after such in-
8 cidents or crises.

9 (D) Utilization of modeling, simulation,
10 and analysis under subparagraph (A) to provide
11 recommendations to policymakers, and to de-
12 partments and agencies of the Federal Govern-
13 ment and private sector persons and entities
14 upon request, regarding means of enhancing the
15 stability of, and preserving, critical infrastruc-
16 tures.

17 (3) RECIPIENT OF CERTAIN SUPPORT.—Mod-
18 eling, simulation, and analysis provided under this
19 subsection shall be provided, in particular, to rel-
20 evant Federal, State, and local entities responsible
21 for critical infrastructure protection and policy.

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

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

4 (f) AUTHORIZATION OF APPROPRIATIONS.—There is
5 hereby authorized for the Department of Defense for fiscal
6 year 2002, \$20,000,000 for the Defense Threat Reduction
7 Agency for activities of the National Infrastructure Sim-
8 ulation and Analysis Center under this section in that fis-
9 cal year.

Passed the House of Representatives October 24,
2001.

Attest:

JEFF TRANDAHL,

Clerk.