SENATE BILL 1251
By Akbari

HOUSE BILL 1465

By Towns

AN ACT to amend Tennessee Code Annotated, Title 4; Title 38; Title 39; Title 54; Title 58 and Title 65, relative to critical infrastructure.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF TENNESSEE:

SECTION 1. Tennessee Code Annotated, Title 38, is amended by adding the following as a new chapter:

38-15-101. Short title.

This chapter is known and may be cited as the "Critical Infrastructure Identification, Prioritization, and Protection Act."

38-15-102. Purpose and findings.

(a) The general assembly finds that:

(1) This state's open and technologically complex society includes a wide array of critical infrastructure and key resources that are potential terrorist targets. The majority of these are owned and operated by the private sector and state or local governments. These critical infrastructures and key resources are both physical and cyber-based and span all sectors of the economy;

(2) Critical infrastructure and key resources provide the essential services that underpin our society. This state possesses numerous key resources, the exploitation or destruction of which by terrorists could cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction, or could profoundly affect our morale. In addition, there is critical infrastructure so vital that its incapacitation, exploitation,

or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being; and

(3) While it is not possible to protect or eliminate the vulnerability of all critical infrastructure and key resources throughout the state, strategic improvements in security can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur. In addition to strategic security enhancements, tactical security improvements can be rapidly implemented to deter, mitigate, or neutralize potential attacks.

(b) In accordance with the findings described under subsection (a), this chapter establishes a state policy for departments, agencies, and political subdivisions to identify and prioritize critical infrastructure and key resources and to protect them from terrorist attacks.

38-15-103. Definitions.

For purposes of this chapter:

(1) "Commissioner" means the commissioner of safety;

(2) "Critical infrastructure":

(A) Means systems and assets, whether physical or virtual, so vital to this state, or a political subdivision of the state, that the incapacity or destruction of such systems and assets would have a debilitating impact on physical security, economic security, public health or safety, or any combination of those matters; and

(B) Includes, but is not limited to, the infrastructure of the following services to the general public:

(i) Telephone, television, internet, or other telecommunication services;

(ii) Electric, heat, natural gas, or other power or energy services;

(iii) The distribution of crude or refined liquid petroleum products or natural gas, and the pipelines, pumping stations, terminals, and equipment necessary for operation of the facility;

(iv) Water, wastewater, or sewer services; and

(v) Railroads and other transportation services;

(3) "Department" means the department of safety;

(4) "Homeland security council" or "council" means the homeland security council created by Executive Order No. 8 of 2003 within the department of safety;

(5) "Key resources" mean publicly or privately controlled resources essential to the minimal operations of the economy and government; and

(6) "Sector-specific agency" means a state department or agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category and that conducts its activities under this chapter in accordance with guidance provided by the department and the homeland security council.

38-15-104. Policy – Department and agency requirements.

(a) It is the policy of this state to enhance the protection of the state's critical infrastructure and key resources against terrorist acts that could:

(1) Cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction;

(2) Impair state departments' and agencies' abilities to perform essential missions, or to ensure the public's health and safety;

(3) Undermine state and local government capacities to maintain order and to deliver minimum essential public services;

(4) Damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services;

(5) Have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources; or

(6) Undermine the public's morale and confidence in the state's economic and political institutions.

(b) State departments and agencies shall:

(1) Identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. Departments and agencies shall consult with federal departments and agencies, local governments, and the private sector to accomplish this objective;

(2) Ensure that homeland security programs do not diminish the overall economic security of this state;

(3) Appropriately protect information associated with carrying out this chapter, including handling voluntarily provided information and information that would facilitate terrorist targeting of critical infrastructure and key resources consistent with the federal Homeland Security Act of 2002 (Pub. L. No. 107-296) and other applicable legal authorities; and

(4) Implement this chapter in a manner that protects the rights of this state's residents.

38-15-105. Roles and responsibilities of the department and commissioner.

(a) To effectuate the purposes of this chapter, the commissioner shall coordinate, in consultation with the homeland security council, the overall state effort to enhance the protection of the critical infrastructure and key resources of this state. The commissioner shall serve as the principal state official to lead, integrate, and coordinate implementation of efforts among state departments and agencies, the federal and local governments, and the private sector to protect critical infrastructure and key resources.

(b) Consistent with the responsibilities established in subsection (a), the commissioner shall identify, prioritize, and coordinate the protection of critical infrastructure and key resources with an emphasis on critical infrastructure and key resources that could be exploited to cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction.

(c) The commissioner shall establish uniform policies, approaches, guidelines, and methodologies for integrating infrastructure protection and risk management activities within and across sectors along with metrics and criteria for related programs and activities.

(d) The department, in consultation with the homeland security council, shall coordinate protection activities for each of the following critical infrastructure sectors:

(1) Information technology;

(2) Telecommunications; and

(3) Emergency services.

(e) The department, in consultation with the homeland security council, shall coordinate with appropriate departments and agencies to ensure the protection of other key resources including dams, government facilities, and commercial facilities.

38-15-106. Roles and responsibilities of the homeland security council and other departments and agencies.

(a) The homeland security council shall evaluate the need for and make recommendations to the commissioner regarding coverage of additional critical infrastructure and key resources categories over time, as appropriate.

(b) Recognizing that each infrastructure sector possesses its own unique characteristics and operating models, the following sector-specific agencies shall identify, and make recommendations regarding, critical infrastructure and key resource protection needs to the homeland security council:

(1) Department of agriculture;

(2) Department of health;

(3) Department of environment and conservation;

(4) Department of transportation;

(5) Department of finance and administration;

(6) Department of military;

(7) Tennessee emergency management agency; and

(8) Tennessee public utilities commission.

(c) In identifying, and making recommendations regarding, critical infrastructure and key resource protection needs, the council and sector-specific agencies should collaborate with relevant federal departments and agencies, local governments, and the private sector, including with key persons and entities in their infrastructure sector; conduct or facilitate vulnerability assessments of the sector; and encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.

SECTION 2. The headings in this act are for reference purposes only and do not constitute a part of the law enacted by this act. However, the Tennessee Code Commission is requested to include the headings in any compilation or publication containing this act.

SECTION 3. This act takes effect upon becoming a law, the public welfare requiring it.