WEST VIRGINIA LEGISLATURE
SEVENTY-EIGHTH LEGISLATURE
REGULAR SESSION, 2007

ENROLLED
COMMITTEE SUBSTITUTE
FOR
Senate Bill No. 386

(Senators Boley and Love, original sponsors)

[Passed March 10, 2007; in effect ninety days from passage.]
AN ACT to amend and reenact §29B-1-4 of the Code of West Virginia, 1931, as amended, relating to exempting from public disclosure specific engineering plans of existing public utility plants and equipment; and exempting customer proprietary network information from public disclosure of information, consistent with federal law.

Be it enacted by the Legislature of West Virginia:
That §29B-1-4 of the Code of West Virginia, 1931, as amended, be amended and reenacted to read as follows:

ARTICLE 1. PUBLIC RECORDS.

§29B-1-4. Exemptions.

(a) The following categories of information are specifically exempt from disclosure under the provisions of this article:

(1) Trade secrets, as used in this section, which may include, but are not limited to, any formula, plan pattern, process, tool, mechanism, compound, procedure, production data or compilation of information which is not patented which is known only to certain individuals within a commercial concern who are using it to fabricate, produce or compound an article or trade or a service or to locate minerals or other substances, having commercial value, and which gives its users an opportunity to obtain business advantage over competitors;

(2) Information of a personal nature such as that kept in a personal, medical or similar file, if the public disclosure thereof would constitute an unreasonable invasion of privacy, unless the public interest by clear and convincing evidence requires disclosure in the particular instance: *Provided*, That nothing in this article shall be construed as precluding an individual from inspecting or copying his or her own personal, medical or similar file;

(3) Test questions, scoring keys and other examination data used to administer a licensing examination, examination for employment or academic examination;
(4) Records of law-enforcement agencies that deal with the detection and investigation of crime and the internal records and notations of such law-enforcement agencies which are maintained for internal use in matters relating to law enforcement;

(5) Information specifically exempted from disclosure by statute;

(6) Records, archives, documents or manuscripts describing the location of undeveloped historic, prehistoric, archaeological, paleontological and battlefield sites or constituting gifts to any public body upon which the donor has attached restrictions on usage or the handling of which could irreparably damage such record, archive, document or manuscript;

(7) Information contained in or related to examination, operating or condition reports prepared by, or on behalf of, or for the use of any agency responsible for the regulation or supervision of financial institutions, except those reports which are by law required to be published in newspapers;

(8) Internal memoranda or letters received or prepared by any public body;

(9) Records assembled, prepared or maintained to prevent, mitigate or respond to terrorist acts or the threat of terrorist acts, the public disclosure of which threaten the public safety or the public health;

(10) Those portions of records containing specific or unique vulnerability assessments or specific or unique response plans, data, databases and inventories of goods
or materials collected or assembled to respond to
terrorist acts; and communication codes or deployment
plans of law enforcement or emergency response
personnel;

(11) Specific intelligence information and specific
investigative records dealing with terrorist acts or the
threat of a terrorist act shared by and between federal
and international law-enforcement agencies, state and
local law enforcement and other agencies within the
Department of Military Affairs and Public Safety;

(12) National security records classified under federal
executive order and not subject to public disclosure
under federal law that are shared by federal agencies
and other records related to national security briefings
to assist state and local government with domestic
preparedness for acts of terrorism;

(13) Computing, telecommunications and network
security records, passwords, security codes or programs
used to respond to or plan against acts of terrorism
which may be the subject of a terrorist act;

(14) Security or disaster recovery plans, risk
assessments, tests or the results of those tests;

(15) Architectural or infrastructure designs, maps or
other records that show the location or layout of the
facilities where computing, telecommunications or
network infrastructure used to plan against or respond
to terrorism are located or planned to be located;

(16) Codes for facility security systems; or codes for
secure applications for such facilities referred to in
subdivision (15) of this subsection;

(17) Specific engineering plans and descriptions of existing public utility plants and equipment; and

(18) Customer proprietary network information of other telecommunications carriers, equipment manufacturers and individual customers, consistent with 47 U. S. C. §222.

(b) As used in subdivisions (9) through (16), inclusive, subsection (a) of this section, the term "terrorist act" means an act that is likely to result in serious bodily injury or damage to property or the environment and is intended to:

(1) Intimidate or coerce the civilian population;

(2) Influence the policy of a branch or level of government by intimidation or coercion;

(3) Affect the conduct of a branch or level of government by intimidation or coercion; or

(4) Retaliate against a branch or level of government for a policy or conduct of the government.

(c) Nothing in the provisions of subdivisions (9) through (16), inclusive, subsection (a) of this section should be construed to make subject to the provisions of this chapter any evidence of an immediate threat to public health or safety unrelated to a terrorist act or the threat thereof which comes to the attention of a public entity in the course of conducting a vulnerability assessment response or similar activity.
The Joint Committee on Enrolled Bills hereby certifies that the foregoing bill is correctly enrolled.

Chairman Senate Committee

Chairman House Committee

Originated in the Senate.

In effect ninety days from passage.

Clerk of the Senate

Clerk of the House of Delegates

President of the Senate

Speaker House of Delegates

The within is approved this the Day of 2007.

Governor
PRESENTED TO THE GOVERNOR

APR 03 2007

Time 1:30