PENNSYLVANIA NEWSPAPER ASSOCIATION

House Committee on Veterans Affairs and Emergency Preparedness

House Bill 2562, Printer's No. 3930

Media, PA
August 29, 2012

Chairman Barrar, Chairman Sainato, and members of the Committee: I am Martin Till, publisher of the Express-Times, Easton, PA, and president of Penn-Jersey Advance. On behalf of the Pennsylvania Newspaper Association (PNA), I appreciate the opportunity to share our concerns about proposed changes to Pennsylvania's emergency preparedness law. We must object to the overbroad language of Sec. 7715 providing blanket confidentiality for any record or meeting related to safety, security or emergency preparedness.

As a general matter, we do understand that certain information related to these matters may be confidential, however, these records are already adequately protected under Pennsylvania's Right to Know Law, 65 P.S. 67.101. That law devotes four separate and detailed exemptions to the protection of homeland security, public utility infrastructure, information technology, and personal security information. These are found at 65 P.S. 67.708(b)(1),(2),(3), and (4), attached for your review.

Section 7715(a) of House Bill 2562 gives complete discretion, not subject to appeal, to the Director of PEMA and a host of unidentified individuals working in law enforcement, school districts, municipalities, and state and local emergency agencies to declare virtually any record confidential on the basis of their personal opinion that it is "*reasonably likely to jeopardize or threaten public safety or preparedness or public protection activity.*"

Although this same phrase appears in exception 708(b)(2) of the Right to Know Law, House Bill 2562 omits crucial elements of the Law that were drafted to work in concert with the "reasonable likelihood" standard: the burden of proof to support a contention of confidentiality, which is placed on every agency subject to the Law, and the possibility for a requester to appeal a decision.

The Right to Know Law further requires the evaluation standard to assess the "*substantial and demonstrable risk of physical harm,*" a far more stringent standard than the bill's reference to the possibility of a threat. Moreover, the Right to Know Law makes it clear that the burden of proof is on an agency seeking to deny access to a public record. Pennsylvania's Commonwealth Court affirmed this in the case of Bowling vs. Office of Open Records, which addressed a denial by PEMA of a request for records of goods and services purchased with federal grant funds.

PEMA had attempted to block access to all such records, an act that the Court did not permit. The Court ruled against blanket redactions in that case, requiring PEMA or any agency, in its response to a request for a record, to identify how the item that was purchased fits into one of the Law's exemptions. They considered computer server locations to be a reasonable redaction under the Right to Know Law, but not bungee cords.

Although Section 7715(a) tracks some of the language of 65 P.S. 67.708(b)(2), House Bill 2562 is also at odds with the Right to Know Law's acknowledgement that financial records are public. Section 708(c) of the Right to Know Law permits agencies to redact certain security-related information from financial records, but requires agencies to produce the remainder of the record.

Finally, Section 7715(b) would make all meetings relating to preparedness and emergency management closed to the public. This is overbroad and inappropriate. Meetings of government agencies should be presumptively open, and should only be closed when holding an open discussion would threaten public safety or preparedness. Otherwise, it becomes far too easy for government to operate out of the public's view.

Pennsylvania's experience in 2010 with the Office of Homeland Security's contract with the Institute for Terrorism Research and Response (ITRR) provides ample illustration of the need for public oversight and accountability, even with regard to homeland security and emergency preparedness. You'll recall that the ITRR produced "security bulletins" on organizations and events that they deemed potentially troublesome.

It turned out, however, that people who were merely exercising their democratic rights had been targeted, and surveillance was conducted on such disparate groups as animal rights' organizations, gay activists, and people who were protesting natural gas drilling. ITRR sent those bulletins to the Pennsylvania State Police and PEMA, and they could have easily been deemed "confidential" under the current drafting of Sec. 7715.

In sum, safety and security-related records are well protected in the new Right to Know Law, which was reviewed and debated at length before taking effect only three and one half years ago. House Bill 2562 could shield a wide array of information about which the public needs to know, including evidence of financial wrongdoing, wasteful spending, or environmental hazards.

Without evaluation criteria or appeal of a decision under the process established in the Right to Know Law, these amendments to Title 35 would constitute a significant step backward, in a crucial area of government activity. As drafted, the bill before you would render decisions made by every local official and staff member – even volunteer firefighters - immune to any challenge or appeal, as long as certain key phrases appear in their response to a request. That change itself would be both unique and unprecedented in our democracy.

If open government is to mean anything in Pennsylvania, it starts with the proposition that government records and meetings are open. The very comprehensive exceptions already found in state as well as Federal law are more than adequate to protect the public. We respectfully urge you to remove Sec. 7715 from this legislation, and look forward to working with you on this important bill.

Attachment

Attachment A

Act 3- 2008, the Right to Know Law
Safety and Security Exception; 65 P.S. Sec. 708(b)(1),(2),(3),(4)

The following are exempt from access by a requester under this act:

(1) A record the disclosure of which:

(i) would result in the loss of Federal or State funds by an agency or the Commonwealth; or

(ii) would be reasonably likely to result in a substantial and demonstrable risk of physical harm to or the personal security of an individual.

(2) A record maintained by an agency in connection with the military, homeland security, national defense, law enforcement or other public safety activity that if disclosed would be reasonably likely to jeopardize or threaten public safety or preparedness or public protection activity or a record that is designated classified by an appropriate Federal or State military authority.

(3) A record, the disclosure of which creates a reasonable likelihood of endangering the safety or the physical security of a building, public utility, resource, infrastructure, facility or information storage system, which may include:

(i) documents or data relating to computer hardware, source files, software and system networks that could jeopardize computer security by exposing a vulnerability in preventing, protecting against, mitigating or responding to a terrorist act;

(ii) lists of infrastructure, resources and significant special events, including those defined by the Federal Government in the National Infrastructure Protections, which are deemed critical due to their nature and which result from risk analysis; threat assessments; consequences assessments; antiterrorism protective measures and plans; counterterrorism measures and plans; and security and response needs assessments; and

(iii) building plans or infrastructure records that expose or create vulnerability through disclosure of the location, configuration or security of critical systems, including public utility systems, structural elements, technology, communication, electrical, fire suppression, ventilation, water, wastewater, sewage and gas systems.

(4) A record regarding computer hardware, software and networks, including administrative or technical records, which, if disclosed, would be reasonably likely to jeopardize computer security.

****

/PNA 8.29.12