Ohio's Public Records Act
R.C. 149.43 and 149.433
(current "Yellow Book" can be found at
www.ohioattorneygeneral.gov/Legal/Sunshine Laws/Publications/
2009 Sunshine Laws Manual)

The Federal Emergency Planning and Community Right-To-Know Act
42 U.S.C. §1101, et seq.

Ohio's Emergency Planning Statute
R.C. Chapter 3750

Ohio Constitution
Article XVIII, §3
(Home Rule)

Updated: August 13, 2009

Ohio's Public Records Act

Records in the files of the State Emergency Response Commission (SERC) and the Local Emergency Planning Committees (LEPCs) are governed by Ohio's Public Records Act, R.C. Chapter 149.43. However, R.C. 149.43 (A)(1)(v) – the "catch-all exception" – provides the following prohibition regarding the release of public records: Records the release of which is prohibited by state or federal law.

Federal law, the Emergency Planning and Right-to-Know Act (EPCRA) and state law, R.C. Chapter 3750 (Ohio's Emergency Planning statute) set forth various requirements regarding the availability and release of public records maintained in the files of SERC and the LEPCs. Thus, these requirements need to be followed when SERC and the LEPCs receive a public document request.

HOWEVER, to the extent an EPCRA and R.C. Chapter 3750 requirement does not address the availability and release of public records maintained in the files of SERC and the LEPCs, the requirements of Ohio's Public Records Act need to be followed. Examples include, posting a public records policy at the public office, prompt inspection of public records, and providing requested copies in a reasonable time.

The Federal Emergency Planning and Community Right-To-Know Act

42 U.S.C. §1101

(a) Establishment of State emergency response commissions. Not later than six months after October 17, 1986, the **Governor of each State shall appoint a State emergency response commission**. The Governor may designate as the State emergency response commission one or more existing emergency response organizations that are State-sponsored or appointed. The Governor shall, to the extent practicable, appoint persons to the State emergency response commission who have technical expertise in the emergency response field. **The State emergency response commission shall appoint local emergency planning committees under subsection (c) of this section and shall supervise and coordinate the activities of such committees. The State emergency response commission shall establish procedures for receiving and processing requests from the public for information under section 11044 of this title, including tier II information under section 11022 of this title. Such procedures shall include the designation of an official to serve as coordinator for information.** If the Governor of any State does not designate a State emergency response commission within such period, the Governor shall operate as the State emergency response commission until the Governor makes such designation. (emphasis added).

[Federal statutory mandate which requires establishment of Ohio's SERC and Ohio's LEPCs and which requires the availability and release of public records maintained in the files of SERC and the LEPCs.]

The Federal Emergency Planning and Community Right-To-Know Act

42 U.S.C. §11044

(a) Availability to public. Each emergency response plan, material safety data sheet, list described in section 11021(a)(2) of this title, inventory form, toxic chemical release form, and followup emergency notice shall be made available to the general public, consistent with section 11042 of this title, during normal working hours at the location or locations designated by the Administrator, Governor, State emergency response commission, or local emergency planning committee, as appropriate. **Upon request by an owner or operator of a facility subject to the requirements of section 11022 of this title, the State emergency response commission and the appropriate local emergency planning committee shall withhold from disclosure under this section the location of any specific chemical required by section 11022(d)(2) of this title to be contained in an inventory form as tier II information**. (emphasis added).

[Federal statutory mandate regarding the public availability of SERC and the LEPC files. Also, provides that upon the request of a facility, chemical storage location information contained in the inventory form is to be kept confidential.]

Ohio's Emergency Planning Statute
R.C. Chapter 3750

R.C. 3750.02

(B) The commission shall:

(1) Adopt rules in accordance with Chapter 119. of the Revised Code that are consistent with and equivalent in scope, content, and coverage to the "Emergency Planning and Community Right-To-Know Act of 1986," 100 Stat. 1729, 42 U.S.C.A. 11001, and applicable regulations adopted under it:

(i) Establishing criteria and procedures to protect trade secret and confidential business information from unauthorized disclosure;

[The rules adopted by SERC to protect trade secret and confidential business information from unauthorized disclosure are set forth in Ohio Administrative Code Chapter 3750-60.]

(2) Adopt rules in accordance with Chapter 119. of the Revised Code to implement and administer this chapter that may be more stringent than the "Emergency Planning and Community Right-To-Know Act of 1986," 100 Stat. 1729, 42 U.S.C.A. 11001, and regulations adopted under it. Rules adopted under division (B)(2) of this section shall not be inconsistent with that act or the regulations adopted under it. The rules shall:

(c) Establish policies and procedures for maintaining information submitted to the commission and local emergency planning committees under this chapter, and for receiving and fulfilling requests from the public for access to review and to obtain copies of that information. The criteria and procedures shall include the following requirements and authorizations regarding that information and access to it:

(i) Information that is protected as trade secret information or confidential business information under this chapter and rules adopted under it shall be kept in files that are separate from those containing information that is not so protected.

(ii) The original copies of information submitted to the commission or committee shall not be removed from the custody and control of the commission or committee.

(iii) A person who, either in person or by mail, requests to obtain a copy of a material safety data sheet submitted under this chapter by a facility owner or operator shall submit a separate application for each facility for which a material safety data sheet is being requested.

(iv) A person who requests to receive by mail a copy of information submitted under this chapter by a facility owner or operator shall submit a separate application for each facility for which information is being requested and shall specify both the facility for which information is being requested and the particular types of documents requested.

(v) Only employees of the commission or committee shall copy information in the files of the commission or committee.

(vi) The commission or committee may require any person who requests to review or obtain a copy of information in its files to schedule an appointment for that purpose with the information coordinator of the commission or committee at least twenty-four hours before arriving at the office of the commission or committee for the review or copy.

(vii) Any person who seeks access to information in the files of the commission or a local emergency planning committee shall submit a written application, either in person or by mail, to the information coordinator on a form provided by the commission or committee. The person also shall provide the person's name and current mailing address on the application and may be requested by the commission or committee to provide basic demographic information on the form to assist in the evaluation of the information access provisions of this chapter and rules adopted under it. Application forms may be obtained by mail or in person or by request by telephone at the office of the commission or committee during regular business hours. Upon receipt of a request for an application by telephone or

mail, the information coordinator shall promptly mail an application to the person who requested it.

(viii) The application form shall provide the applicant with a means of indicating that the applicant's name and address are to be kept confidential. If the applicant so indicates, that information is not a public record under section 149.43 of the Revised Code and shall not be disclosed to any person who is not a member or employee of the commission or committee or an employee of the environmental protection agency. When a name and address are to be kept confidential, they also shall be deleted from the copy of the application required to be placed in the file of the facility under division (B)(2)(c)(xii) of this section and shall be withheld from any log of information requests kept by the commission or committee pursuant to that division.

[The requirements for a written application and name and address of the applicant for information are requirements that are NOT set forth in Ohio's Public Records Act. Requests for public records pursuant to Ohio's Public Records Act can be verbal, and there is no requirement to provide name and address. However, as set forth above, if the applicant requests his/her name and address to be kept confidential, SERC and the LEPCs must keep this information confidential.]

(ix) Neither the commission nor a local emergency planning committee shall charge any fee for access to review information in its files when no copies or computer searches of that information are requested.

(x) An applicant shall be informed of the cost of copying, mailing, or conducting a computer search of information on file with the commission or committee before such a copy or search is made, and the commission or committee shall collect the appropriate fees as established under section 3750.13 of the Revised Code. Each applicant shall acknowledge on the application form that the applicant is aware that the applicant will be charged for copies and computer searches of that information the applicant requests and for the costs of mailing copies of the information to the applicant.

[Consistent with Ohio's Public Records Act, SERC and the LEPCs can charge the applicant the cost of copying, mailing, or conducting a computer search, but SERC and the LEPCs must comply with Ohio's Public Records Act which prohibits charges for employee time responding to the request for records.]

(xi) The commission or committee may require a person requesting copies of information on file with it to take delivery of them in the office of the commission or committee whenever it considers the volume of the information to be large enough to make mailing or delivery by a parcel or package delivery service impractical.

(xii) When the commission or committee receives a request for access to review or obtain copies of information in its files, it shall not routinely notify the owner or operator of the facility involved, but instead shall either keep a log or file of requests for the information or shall place a copy of each completed application form in the file for the facility to which the application pertains. Such a log or file shall be available for review by the public and by the owners and operators of facilities required to submit information to the commission or committee under this chapter and rules adopted under it.

(8) Adopt rules in accordance with Chapter 119. of the Revised Code establishing reasonable maximum fees that may be charged by the commission and local emergency planning committees for copying information in the commission's or committee's files to fulfill requests from the public for that information;

(12) Designate an officer of the environmental protection agency to serve as the commission's information coordinator under this chapter;

R.C. 3750.03

(D) A local emergency planning committee shall:

(3) Appoint an information coordinator who shall be responsible for maintaining the committee's files of information received under this chapter and rules adopted under it and for receiving and fulfilling requests from the public for that information;

R.C. 3750.10

(A) Any person who seeks to review or obtain copies of information submitted to the emergency response commission or a local emergency planning committee under this chapter and rules adopted under it shall submit a written application to the information coordinator of the commission or committee in accordance with the policies and procedures in rules adopted under division (B)(2)(c) of section 3750.02 of the Revised Code. Upon submission of a completed application, the information coordinator shall provide the applicant access to or copies of the information requested, or shall perform the requested computer search and provide the applicant with the information obtained from it, in accordance with those policies and procedures, subject to the restrictions under division (B)(5) of this section on the release of information on emergency and hazardous chemical inventory forms submitted under section 3750.08 of the Revised Code that is designated as tier II information and to the restrictions on the disclosure of trade secret and confidential business information established

in rules adopted under division (B)(1)(i) of section 3750.02 of the Revised Code.

(B)(1) Upon receiving the written request of an officer or employee of the state or a political subdivision acting in his official capacity, the commission or committee shall make available to the officer or employee an emergency and hazardous chemical inventory form that contains tier II information. If the commission or committee does not have the requested inventory form containing that information, it shall request the owner or operator of the facility to submit one. The owner or operator of the facility shall submit the requested inventory form to the commission or committee within thirty days after receiving the request to submit it. Upon receipt of the requested inventory form, the commission or committee shall provide it to the public officer or employee who requested it, subject to the restrictions on the disclosure of trade secret and confidential business information established in rules adopted under division (B)(1)(i) of section 3750.02 of the Revised Code.

(2) Upon receiving an application from any person to review or obtain a copy of an emergency and hazardous chemical inventory form containing tier II information that is in the possession of the commission or committee, the commission or committee shall provide the applicant access to review the form or obtain a copy of it in accordance with the policies and procedures established in rules adopted under division (B)(2)(c) of section 3750.02 of the Revised Code, subject to the restrictions under division (B)(5) of this section on the release of information on emergency and hazardous chemical inventory forms designated as tier II information and to the restrictions on the disclosure of trade secret and confidential business information established in rules adopted under division (B)(1)(i) of section 3750.02 of the Revised Code.

(3) If the commission or committee does not have the requested inventory form containing tier II information and if the requested inventory form pertains to a hazardous chemical that was present at the facility in an amount equal to or exceeding ten thousand pounds at any time during the preceding calendar year, the commission or committee shall request the owner or operator of the facility to submit an emergency and hazardous chemical inventory form containing tier II information regarding the hazardous chemical. The owner or operator of the facility shall submit the requested inventory form to the commission or committee within thirty days after

receiving the request to submit it. Upon receiving the requested inventory form, the commission or committee shall provide access to review it or a copy of it to the applicant in accordance with the policies and procedures established in rules adopted under division (B)(2)(c) of section 3750.02 of the Revised Code, subject to the restrictions under division (B)(5) of this section on the release of information on emergency and hazardous chemical inventory forms designated as tier II information and to the restrictions on the disclosure of trade secret and confidential business information established in rules adopted under division (B)(1)(i) of section 3750.02 of the Revised Code.

(4) If the commission or committee does not have the requested inventory form containing tier II information and if the requested inventory form pertains to a hazardous chemical that was present at the facility in an amount less than ten thousand pounds at any time during the preceding calendar year, the person's application for access to review or obtain a copy of the inventory form shall contain the person's statement of general need for the information, in addition to the other information required on the application form. If the commission or committee finds that the applicant's statement of general need for the information constitutes a valid need for it under rules adopted pursuant to division (B)(1)(g) of section 3750.02 of the Revised Code, the commission or committee shall request the owner or operator of the facility to submit an inventory form that contains tier II information pertaining to the hazardous chemical. The owner or operator of the facility shall submit the requested inventory form to the commission or committee within thirty days after receiving the request to submit it. Upon receiving the requested inventory form, the commission or committee shall provide access to review it or a copy of it to the applicant in accordance with the policies and procedures established in rules adopted under division (B)(2)(c) of section 3750.02 of the Revised Code, subject to the restrictions on the release of tier II information in division (B)(5) of this section and to the restrictions on the disclosure of trade secret and confidential business information established in rules adopted under division (B)(1)(i) of section 3750.02 of the Revised Code.

(5) The owner or operator of a facility may request in writing that the storage location of a hazardous chemical at a facility provided on an emergency and hazardous chemical inventory form containing tier II information submitted under this section or section 3750.08 of the Revised Code not be disclosed to any person who is not an officer or employee of the

state or a political subdivision acting in his official capacity. If the owner or operator of a facility has submitted such a request to the commission or a committee, the commission or committee shall not disclose information concerning the specific storage location of the hazardous chemical at the facility to any person who is not an officer or employee of the state or a political subdivision acting in his official capacity.

[State statutory provision implementing the EPCRA requirement that upon the request of a facility, chemical storage location information contained in the inventory form is to be kept confidential. Copy of inventory form attached.]

(C) No owner or operator of a facility where a hazardous chemical is stored, handled, or processed in an amount that exceeds the threshold quantity for the hazardous chemical established in rules adopted under division (B)(1)(b) or (C)(5) of section 3750.02 of the Revised Code shall fail to submit an emergency and hazardous chemical inventory form containing tier II information in compliance with division (A) or (B) of this section when requested to do so under either of those divisions.

Exceptions, Exceptions, Exceptions . . .What good law does not have them.

R.C. 3750.22

(A)(1) The owner or operator of a facility where chemicals are produced, or the owner or operator of any other facility or business of any type, ***may provide*** **a copy of any vulnerability assessment of the facility or business or of any other security-sensitive information** developed regarding the facility or business to any of the following:

(a) The local emergency planning committee of the emergency planning district in which the facility or business is located;

(b) The fire department with jurisdiction over the facility or business;

(c) The sheriff of the county in which the facility or business is located;

(d) The chief of police of any municipal corporation with jurisdiction over the facility or business;

(e) Any state agency involved in the development of plans to protect businesses of any type against terrorist attack including the Ohio department of public safety, the Ohio highway patrol, the office of homeland security, and the emergency management agency.

(2) A local emergency planning committee, fire department, sheriff, or chief of police, or other public office that receives a vulnerability assessment or other security-sensitive information pursuant to division (A)(1) of this section may provide a copy of that assessment or information to any local emergency planning committee, fire department, sheriff, or chief of police, or other public office described in division (A)(1) of this section but shall not share that vulnerability assessment or security-sensitive information with any other public or private office unless required to do so by federal or state law.

(B)(1) **Any vulnerability assessment or other security-sensitive information a public office *receives* pursuant to division (A) of this section is not a public record under section 149.43 of the Revised Code**

and that assessment or information is not subject to the mandatory disclosure requirements of section 149.43 of the Revised Code.

(2) This section shall not be construed to exempt any owner or operator of a facility where chemicals are produced or the owner or operator of any other facility or business of any type from providing information contained in a vulnerability assessment or other security-sensitive information to the public when the provision of that information otherwise is required by federal or state law. (emphasis added).

[Vulnerability assessment discussion:

Vulnerability assessments, or other security-sensitive information, are site security plans, prepared by a facility or business, that describe the appropriate levels of security measures needed to address security vulnerabilities at the facility or business.

Thus, if a facility or business has developed a plan that identifies security vulnerabilities at its site and the measures that would be taken to address a breach of security, for example a terrorist attack, such plans, if submitted to a LEPC, are not subject to disclosure as public records.

Vulnerability assessments, or other security-sensitive information, are not the following documents kept in the LEPC's files;

- **the public information on the Tier II form**
- **material safety data sheets or chemical lists**
- **inventory forms**
- **toxic chemical release forms**

and

- **the emergency response plan prepared by the LEPC**

These documents are subject to disclosure as public documents. Of course if a vulnerability assessment or other security-sensitive information, prepared by the facility or business,
has been incorporated into the emergency response plan that portion of the plan should not be disclosed.]

See attached:

April 27, 2005 Testimony in support of Senate Bill 9, presented by Jack Pounds, President, Ohio Chemistry Technology Council

May 5, 2005 letter from Jack Pounds to Jack Shaner, Ohio Environmental Council

April 9, 2007 Federal Register, Vol. 72, No. 67, pages 17688 and 17702 through17706

R.C. 149.433

(A) As used in this section:

(1) **"Act of terrorism" has the same meaning as in section 2909.21 of the Revised Code.**

(2) "Infrastructure record" means any record that discloses the configuration of a public office's or chartered nonpublic school's critical systems including, but not limited to, communication, computer, electrical, mechanical, ventilation, water, and plumbing systems, security codes, or the infrastructure or structural configuration of the building in which a public office or chartered nonpublic school is located. "Infrastructure record" does not mean a simple floor plan that discloses only the spatial relationship of components of a public office or chartered nonpublic school or the building in which a public office or chartered nonpublic school is located.

(3) "Security record" means any of the following:

(b) **Any record assembled, prepared, or maintained by a public office or public body to prevent, mitigate, or respond to acts of terrorism, including any of the following:**

(i) **Those portions of records containing specific and unique vulnerability assessments or specific and unique response plans either of which is intended to prevent or mitigate acts of terrorism**, and

communication codes or deployment plans of law enforcement or emergency response personnel;

[Security record discussion:

The exclusion provided by R.C. 149.433 excludes from disclosure any record *assembled or prepared by a public office* to prevent, mitigate, or respond to acts of terrorism. As set forth in section (A)(3)(b)(1) the records that are excluded from disclosure are *"specific and unique vulnerability assessments"* or *"specific and unique response plans"* either of which is intended to prevent or mitigate acts of terrorism, and communication codes or deployment plans of law enforcement or emergency response personnel."

R.C. 2909.21(A) defines "acts of terrorism" as an act that is committed within or outside the territorial jurisdiction of this state or the United States, that constitutes a specified offense if committed in this state or constitutes and offense in any jurisdiction within or outside the territorial jurisdiction of the United States containing all of the essential elements of a specified offense, and that is intended to do one or more of the following: (1) Intimidate or coerce a civilian population; (2) Influence the policy of any government by intimidation or coercion; (30 Affect the conduct of any government by the act that constitutes the offense.]

See attached:

S.B. 258 Bill Summary, pages 6-8
2009 "Yellow Book" page 45

Ohio Constitution
Article XVIII, §3
(Home Rule)

Municipalities shall have authority to exercise all powers of local self-government and to adopt and enforce within their limits such local police, sanitary and other similar regulations, as are not in conflict with general laws.

Ohio State Emergency Response Commission
c/o Ohio EPA, Lazarus Government Center
P.O. Box 1049, 122 South Front St.
Columbus, Ohio 43216-1049

STAPLE

Emergency and Hazardous Chemical Inventory Form

Page ___ of ___ Pages

4.1 Facility Name | City | County

Exact Street Location (no box #'s) | Zip Code

4.2 For Filing Date: 03/ 01/ ____

4.3 ☐ Check here if form and FACILITY MAP are Confidential and print "CONFIDENTIAL FORM" here: _____

4.4 ☐ Check if Revision

4.5 ☐ I Have Attached a Facility Map

5.0 Chemical Description										Hazard Class					Location of Chemicals						Amount			
	CAS REGISTRY NO.	SPECIFIC CHEMICAL NAME	PURE	MIXTURE	COMPONENTS	EHS CHEMICAL	SOLID	LIQUID	GAS	TRADE SECRET	ACUTE	CHRONIC	FIRE	REACTIVE	RELEASE OF PRESSURE	B, T, OR A BUILDING, TANK OR AREA NO.	DIVISION OR ROOM LETTER	FLOOR	STORAGE TYPE CODE	PRESSURE & TEMPERATURE CONDITIONS	LOCATION-CONFIDENTIAL	MAXIMUM	AVERAGE	UNITS	NO. OF DAYS ON SITE
1																									
2																									
3																									
4																									
5																									

CERTIFICATION *(READ AND SIGN AFTER COMPLETING ALL SECTIONS)*
I CERTIFY UNDER PENALITY OF LAW THAT I HAVE PERSONALLY EXAMINED AND AM FAMILIAR WITH THE INFORMATION SUBMITTED IN PAGES ONE THROUGH _____, AND THAT BASED ON MY INQUIRY OF THOSE INDIVIDUALS RESPONSIBLE FOR OBTAINING THE INFORMATION, I BELIEVE THAT THE INFORMATION IS TRUE, ACCURATE, AND COMPLETE.

NAME AND OFFICIAL TITLE OF OWNER OR OWNERS AUTHORIZED REPRESENTATIVE | SIGNATURE | DATE SIGNED

OHIO CHEMISTRY TECHNOLOGY COUNCIL

The voice of Ohio's high-tech chemistry community . . .
making a better world for all Ohioans

88 E. Broad Street, Suite 1490 Columbus, Ohio 43215 (614) 224-1730 Fax: (614) 224-5168
www.ohiochemistry.org

Testimony in Support of Senate Bill 9
(Terrorism)

Presented by Jack R. Pounds
President
Ohio Chemistry Technology Council

Before Committee on Transportation, Public Safety, and Homeland Security
Ohio House of Representatives
Wednesday, April 27, 2005

Thank you, Chairman Reinhard- and members of the committee. I am Jack Pounds, President of the Ohio Chemistry Technology Council—the statewide trade association for Ohio's manufacturers and marketers of the products of chemistry. Our organization's membership is composed of some 80 companies, including small, medium, and large companies involved in the research and development, commercialization, production, sale, and distribution of chemical products.

I appreciate the opportunity this afternoon to offer our organization's support for Substitute Senate Bill 9, which contains a number of provisions that complement existing initiatives by the Federal government and the chemical industry to address the threat to the public posed by terrorists attempting to use chemicals and chemical plants as weapons.

Since the attacks of September 11, 2001, our industry has taken action to improve security at the more than 2,000 chemical facilities operated by members of the American Chemistry Council—including more than 120 such sites here in Ohio. Each of these sites has undertaken security vulnerability assessments, implemented security enhancements, and participated in security plan verifications conducted by independent parties. Vital to these industry efforts have been close working relationships with local law enforcement and emergency response officials. In addition, companies in the industry have implemented enhanced security measures that address transportation of hazardous materials and the screening of potential purchasers of hazardous chemicals.

We believe Senate Bill 9 complements these security initiatives in several ways.

- First, the legislation recognizes the International Chemical Weapons Convention's schedules of chemical weapons and precursors as the definitive list of compounds that would be illegal under Ohio law to be in the possession of any party not conforming to the reporting and inspection requirements of the Chemical Weapons Treaty signed by the U.S. and some 190 other nations.

- Second, we support the legislation's criminalization of the intentional use of any hazardous chemical for purposes of terrorism.

- Third, we support the provision in the bill that protects from public disclosure a limited number of sensitive documents, including security vulnerability assessments and security plans developed by private businesses. The bill will allow companies to share in confidence such documents with law enforcement, homeland security, and emergency response personnel for purposes of coordinating anti-terrorist efforts. This protection is very limited, and it does not in any way preempt the public right to know disclosure obligations of businesses who make or use hazardous chemicals. For example, nothing in the bill relieves a company from filing annual hazardous materials inventory reports with local agencies, or from filing annual chemical emissions reports, or from providing "worst case" accident scenario information to government officials and the public.

- Fourth, we strongly support the bill's provisions that make it a crime to harm people or damage property during an attack on any legitimate research facility.

- Finally, we support the bill's requirement that applicants for hazardous materials endorsements to commercial drivers licenses disclose any support they have given to known terrorist organizations. We believe this is consistent with new U.S. Department of Transportation rules requiring background checks, fingerprinting, and standardized photo identification cards

for all hazardous materials drivers across the United States.

The chemical industry appreciates Senator Jacobson's hard work in putting this legislation together—and we especially appreciate the opportunity he gave to us to have a role in developing the bill.

Mr. Chairman, and members of the committee, I thank you for the opportunity to be here this today.

OHIO CHEMISTRY TECHNOLOGY COUNCIL
The voice of Ohio's high-tech chemistry community. . .making a better world for all Ohioans
88 East Broad Street, Suite 1490 Columbus, Ohio 43215 (614) 224-1730 Fax: (614) 224-5168
www.ohiochemistry.org

May 5, 2005

Mr. Jack Shaner
Ohio Environmental Council
1207 Grandview Ave., Ste. 201
Columbus, OH 43212-3449

Dear Mr. Shaner:

In your testimony yesterday on Senate Bill 9 before the House Committee on Homeland Security, Public Safety, and Transportation, you recommended that the General Assembly mandate public disclosure of security vulnerability assessments and security plans developed by companies in the chemical industry.

I would ask that you reconsider your position for two reasons:

First, and of critical importance in addressing the terrorist threat, is the fact that Senate Bill 9 provides a limited exclusion from public disclosure only for highly-sensitive security documents. We are talking here about documents that have been developed voluntarily by chemical companies for the purposes of (1) identifying their vulnerabilities to terrorist attack and, (2) developing appropriate security plan enhancements to address identified vulnerabilities. The limited exclusion from public disclosure in Senate Bill 9 is intended to encourage these companies to continuing sharing these sensitive vulnerability assessments and security plans with law enforcement and emergency response officials. We view this as a critical tool in assuring a coordinated response to the terrorist threat. But forcing law enforcement and emergency response officials to treat these as public documents would mean terrorists could be given access to critical information for use in planning attacks and thwarting security precautions. This would lead to a total collapse in the existing strong working relationship between industry and Ohio government officials at the local, county, and state levels.

Second, the public already has access to complete information regarding chemical plants and other facilities with chemical inventories in their communities. As you know, existing Federal and state "Right to Know" laws provide for public disclosure of an extensive amount of information regarding hazardous chemicals at facilities in Ohio—including the names of such chemicals, their volumes, their hazardous properties, and other data. In addition, these laws require that facilities annually quantify their emissions to the environment and provide these in reports to Ohio government—which in turn are

accessible to the public. Some facilities with highly hazardous chemicals also must assess "worst case" accident scenarios and share that information with government officials and the public. Moreover, through active Local Emergency Planning Committees in every county in the state, the inventory and "worst case scenario" information is used to develop local emergency plans—a process that is open to the public. Your request to add highly sensitive security information to the volumes of data already available to the public would do nothing to enhance community understanding of a facility—but it most certainly would provide terrorists with valuable intelligence to help in criminal attacks.

I would hope that we can stand united in support of both the public Right to Know and this sensible legislation to encourage private-public coordination in the fight against terrorism.

I would be delighted to discuss this topic with you and your organization at any time.

Sincerely,

Jack R. Pounds
President

Copies:
Hon. Jeff Jacobson, President Pro Tem, Ohio Senate
Hon. Steve Reinhard, Chair, Transportation, Public Safety, Homeland Security, Ohio House
Hon. Jeanine Perry, Ranking Member, Transportation, Public Safety, Homeland Security
Hon. Danny Bubp, Transportation, Public Safety, Homeland Security Committee
Hon. Jim Aslanides, "
Hon. Steve Buehrer, "
Hon. David Evans, "
Hon. James Hoops, "
Hon. Randy Law, "
Hon. Joseph Uecker, "
Hon. John Widowfield, "
Hon. Lorraine Fende, "
Hon. Annie Key, "
Hon. Sylvester Patton, "
Hon. Allan Sayre, "
Hon. Kenneth Morckel, Director, Ohio Dept. of Public Safety

Federal Register

Monday,
April 9, 2007

Part III

Department of Homeland Security

6 CFR Part 27
Chemical Facility Anti-Terrorism Standards; Final Rule

DEPARTMENT OF HOMELAND SECURITY

6 CFR Part 27

[DHS–2006–0073]

RIN 1601–AA41

Chemical Facility Anti-Terrorism Standards

AGENCY: Department Of Homeland Security.

ACTION: Interim final rule.

SUMMARY: The Department of Homeland Security (DHS or Department) issues this interim final rule (IFR) pursuant to Section 550 of the Homeland Security Appropriations Act of 2007 (Section 550), which provided the Department with authority to promulgate "interim final regulations" for the security of certain chemical facilities in the United States.

This rule establishes risk-based performance standards for the security of our Nation's chemical facilities. It requires covered chemical facilities to prepare Security Vulnerability Assessments (SVAs), which identify facility security vulnerabilities, and to develop and implement Site Security Plans (SSPs), which include measures that satisfy the identified risk-based performance standards. It also allows certain covered chemical facilities, in specified circumstances, to submit Alternate Security Programs (ASPs) in lieu of an SVA, SSP, or both.

The rule contains associated provisions addressing inspections and audits, recordkeeping, and the protection of information that constitutes Chemical-terrorism Vulnerability Information (CVI). Finally, the rule provides the Department with authority to seek compliance through the issuance of Orders, including Orders Assessing Civil Penalty and Orders for the Cessation of Operations.

EFFECTIVE DATES: This regulation is effective June 8, 2007, except for Appendix A to part 27. A subsequent final rule document will announce the effective date of Appendix A to Part 27.

Comment related to the addition of Appendix A to part 27 only will be accepted until May 9, 2007.

ADDRESSES: You may submit comments, identified by docket number 2006–0073, by *one* of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Mail:* IP/CSCD/Dennis Deziel, Mail Stop 8100, Department of Homeland Security, Washington, DC 20528–8100.

FOR FURTHER INFORMATION CONTACT: Dennis Deziel, Chemical Security Regulatory Task Force, Department of Homeland Security, 703–235–5263.

SUPPLEMENTARY INFORMATION: This interim final rule is organized as follows: Section I explains the public participation provisions and provides a brief discussion of the statutory and regulatory authority and history; Section II summarizes the changes from the Advance Notice of Rulemaking and discusses the revised rule text; Section III summarizes and responds to the comments the Department received in response to the Advance Notice of Rulemaking; and Section IV contains the regulatory analyses for this interim final rule.

Table of Contents

I. Introduction and Background

A. Public Participation

Interested persons are invited to participate in this rulemaking by submitting written data, views, or arguments on Appendix A of this interim final rule. Comments that will provide the most assistance to DHS in finalizing the Appendix will reference specific chemicals and Screening Threshold Quantities on the list, explain the reason for any recommended change, and include data, information, or authority that support such recommended change.

Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.

Comments that include trade secrets, confidential commercial or financial information, Sensitive Security Information (SSI), or Protected Critical Infrastructure Information (PCII) should not be submitted to the public regulatory docket. Please submit such comments separately from other comments on the rule. Comments containing trade secrets, confidential commercial or financial information, Sensitive Security Information (SSI), or Protected Critical Infrastructure Information (PCII) should be appropriately marked as containing such information and submitted by mail

essential services. The commenter indicated that the creation of tiers would allow facilities to maintain security measures commensurate with risk.

A few commenters suggested that DHS did not provide enough information in the Advance Notice on the number of tiers or on how a tier classification would affect a facility's security requirements. Two industry commenters were concerned that DHS might apply the rule requirements to facilities other than those that pose the highest security risk. Two other commenters believed that the tiering approach is not appropriate for cyber security of control systems. One commenter argued that tiers should include consideration of the transportation of chemicals outside the facility property. Another commenter recommended that DHS should modify the tiers after it receives data from regulated facilities. Another commenter thought that DHS should define "present high levels of security risk" and "high risk" at the end of the RAMCAP process and not at the discretion of the Secretary.

Commenters suggested that tiers should be objective and transparent and should provide flexibility. One industry commenter pointed out that tiering allows DHS to focus on the most important facilities first and believed that DHS should establish a de minimis tier that sets thresholds below which a facility does not have to complete the Top-Screen tool. Two commenters noted that tiering provides an incentive for facilities to eliminate risk.

Some industry commenters and State and local agencies suggested that facilities in higher risk tiers should have more contact with DHS, and that lower-risk facilities should have fewer security layers implemented over a longer period of time, greater discretion, or fewer inspections. One commenter, however, believed there should be no difference in regulatory scrutiny or performance standards between tiers.

Response: The Department agrees with many of the commenters that the risk-based tiering structure will allow DHS to focus its efforts on the highest risk facilities first. To that end, the Department intends to retain the model proposed in the Advance Notice. *See, e.g.*, 71 FR 78276, 78283. In sum, the Department's framework for risk-based tiering will consist of four risk-based tiers of high-risk facilities, ranging from high (Tier 1) to low (Tier 4). The Department will use a variety of factors in determining which tier facilities will be placed, including information about the public health and safety risk, economic impact, and mission critical aspects of the given chemicals and Threshold Quantities (TQ) of the chemicals. The Department considers the methods for determining these tiers to be sensitive anti-terrorism information that may be protected from further disclosure. The types and intensity of security measures (necessary to satisfy the risk-based performance standards in the facility's Site Security Plan) will depend on the facility's tier. The Department will mandate the most rigorous levels of protection and regulatory scrutiny for facilities that present the greatest degree of risk. Finally, pursuant to Section 550(a), it is in the discretion of the Secretary to apply regulatory requirements to those facilities that present high levels of security risk; accordingly, the Department believes it is most appropriate for the Secretary to determine which facilities present high-risk (and not, for example, rely solely on output from the CSAT process).

The Department incorporates the concept of "target attractiveness" into its risk equation. Insofar as it is a fairly subjective element, and that it requires considerable analysis to develop, DHS will not incorporate it into the initial tier assignment process. However, insofar as "target attractiveness" is included in the more detailed Security Vulnerability Assessment component of the regulatory process, and insofar as the final determination of tier placement will be based upon the complete analysis of risk, "target attractiveness" will, in fact, be an important element in tier assignment and subsequent risk management efforts.

C. Security Vulnerability Assessments and Site Security Plans

1. General Comments

Comment: One association requested that DHS encourage, but not require, facilities that are not high-risk to conduct vulnerability assessments as a best practice.

Response: The Department has always encouraged the chemical sector to analyze security vulnerabilities and will continue to do so through voluntary sector efforts even if the site has not been designated as high risk under this rule.

Comment: One commenter requested that DHS define "material modifications," as used in §§ 27.215(c)(3) and 27.225(b)(3), or at least provide examples of circumstances or events that rise to the level of "material modifications."

Response: Material modifications can include a whole host of changes, and for that reason, the Department cannot provide an exhaustive list of material modifications. In general, though, DHS expects that material modifications would likely include changes at a facility to chemical holdings (including the presence of a new chemical, increased amount of an existing chemical, or the modified use of a given chemical) or to site physical configuration, which may (1) substantially increase the level of consequence should a terrorist attack or incident occur; (2) substantially increase a facility's vulnerabilities from those identified in the facility's Security Vulnerability Assessment; (3) substantially effect the information already provided in the facility's Top-Screen submission; or (4) substantially effect the measures contained in the facility's Site Security Plan.

2. Submitting a Site Security Plan

Comment: Several industry commenters recommended changes to the proposed process for notifying facilities to submit SSPs and the timing for submitting the SSPs. A number of commenters believed that the most appropriate person to submit an SSP is a corporate representative with first-hand knowledge of security matters at the facility, rather than an officer of the corporation, as proposed. The comments recommended allowing a corporate security contact, a security manager, or a consultant with delegated authority to submit information on behalf of the corporation. The commenters indicated that, in most instances, members of senior management teams do not have day-to-day detailed knowledge on security issues and, thus, cannot meet the proposed qualifications. One of the commenters added that the proposed regulations appear to limit an organization's flexibility to assign internal responsibilities for various aspects of the regulations. Another commenter suggested that, in addition to notifying a covered facility, the Department should notify the facility's corporate ownership (and/or parent corporation) allowing a multi-facility corporation to prepare and submit a response in an efficient and timely manner.

Response: The goal of this rule is to increase flexibility while embracing security for covered facilities, not to unnecessarily decrease flexibility. The rule obligates the chemical facility to submit the Site Security Plan; however, as used herein, the term chemical facility or facility shall also refer to the owner or operator of the chemical facility. While the owner or operator of

a chemical facility may designate someone to submit the Site Security Plan, the owner or operator is responsible for satisfying all the requirements under this part. Note that the Department has added requirements for submitters in the rule (*see* § 27.200(b)(3)) and that the Department discusses those new requirements in the Rule Provisions discussion of § 27.200. *See* § II(B). Finally, it is presumed that the covered facility is the most appropriate party to notify its parent corporation or other related corporate entities as necessary.

3. Content of Site Security Plans

Comment: One commenter stated that, until some of the initial regulatory elements regarding definition of risk and the establishment of tiers is in place, it would be premature for DHS to publish details on Site Security Plans. Another commenter stated that, based on the consequence assessment, every site should be required to have specific security elements in place that prudently deter, detect, delay, and respond based on their assigned tier level. The commenter also stated that, without some degree of access control and physical security specificity based on tier levels, there will be considerable confusion as to the exact considerations needed to meet Department requirements. Another commenter encouraged DHS to abide by the congressional mandate of Public Law 104–113, as described in OMB Circular A119, and ensure that voluntary consensus codes and standards are used when they are applicable under the rule.

Response: The Department has developed a means of assessing risk and a tiering process as described in §§ 27.205 and 27.220. These methods anticipate, on a risk basis, a certain level of vulnerability for a given tier level. A facility's SSP will describe the appropriate levels of security measures that a facility must implement to address the vulnerabilities identified in their SVA and the risk-based performance standards for their tier. The Department has included risk-based performance standards in this interim final rule and will publish further guidance on the risk-based performance standards. The risk-based standards address, among other things, vulnerabilities under the security concepts of detection, deterrence, delay, and response. Finally, the Department notes that covered facilities may use and cite voluntary consensus codes and standards in their SVAs and SSPs to the extent they are appropriate.

4. Approval of Site Security Plans

Comment: In general, commenters supported the proposed submission and approval processes for SSPs. While one commenter endorsed proposed § 27.240(a)(3) stating that the Department will not disapprove an SSP based on the presence or absence of a particular security measure, another commenter believed that the Department should have the authority to disapprove an SSP if a facility has refused to include a widely-practiced and cost-efficient procedure that can severely reduce the risk posed by a chemical facility. Two commenters requested that the Department inform local law enforcement and first responders when the Department is reviewing an SSP in their community and then inform them whether that plan was accepted or rejected. The commenters stated that the health and safety of responders may well depend upon whether the chemical facility has an adequate SSP.

Response: The Department may not disapprove a Site Security Plan submitted under this Part based on the presence or absence of a particular security measure, as provided in Section 550 of the Homeland Security Appropriations Act of 2007. The Department may disapprove a Site Security Plan that fails to satisfy the risk-based performance standards established in § 27.230.

The Department intends to work closely with local law enforcement and first responders to provide adequate homeland security information to them under this rule.

Comment: One commenter recommended that the Department first complete the SSP review and approval process for Tier 1 facilities, then, after soliciting feedback from the Tier 1 facilities on the process, then proceed in a step-wise fashion to subsequent tiers.

Response: The Department will implement the rule in a phased approach but will not necessarily complete all Tier 1 sites prior to undertaking plan review and approvals with lower-tier chemical facilities as the need arises. This is necessary to make sufficient progress with higher-tier chemical facilities and not only the highest tier.

5. Timing

Comment: One concern raised by an industry association related to DHS's resources for reviewing Security Vulnerability Assessments and providing responses in 20 days. Changes to control systems were suggested for reviews and updates within 7 days or sooner. One commenter agreed with updating SSPs annually, but not Security Vulnerability Assessments. Several commenters suggested the following for updates: every 2–5 years for Tier 1 facilities, 3–5 years for Tier 2, and 3–7 years for Tier 3 and beyond.

Numerous reviewers recommended that the reviews be limited to approximately every three years. Two companies and one industry association wanted reviews to follow major changes and not follow a set schedule. Many reviewers wanted periodic replaced with a suggested frequency.

Several commenters stated that the requirement to submit SVAs within 60 calendar days, and SSPs within 120 calendar days, starting on the date that the facility is notified that it is considered high-risk, is too short, and therefore inadequate. One commenter noted that managing change in a safe fashion requires significant thought and careful planning to ensure that the change itself does not create another hazard to the community, the environment, or employees. The commenter also noted that developing and implementing an SSP that properly mitigates risk requires the security manager to make appropriate revisions to existing facility procedures and to train employees and other affected parties on these new procedures. Another commenter expressed concern that there is no specific date or time by which DHS must notify high-risk chemical facilities of their status. Likewise, there is no firm time by which the Secretary will send out a notice approving or disapproving an SSP.

With regard to the time needed to review an SSP, one commenter stated that DHS should issue a decision approving or disapproving them within 30 days of receipt of a completed plan. This timeframe would bring at least most priority facilities into compliance within seven months of the effective date. The commenter also stated that, given the urgency, any "objections" or "appeals" should be processed after the seven-month schedule is completed. Because of concern that DHS staffing levels might delay the processing of SSPs, another commenter requested a provision be included in the interim final rule indicating that facilities are deemed in compliance after 30 days of submission of SVAs and SSPs until such time that the Department reviews and responds to the submission.

A few commenters recommended that the deadline for Tier 1 facilities to submit SSPs be extended from 120 days to 180 days. The commenters believe that this extension would assure facilities adequate time to assemble the

best teams, prepare thorough SVAs, deal with budget planning for potentially large capital expenditures, and ensure the on-site work is properly conducted. Another commenter agreed that the proposed submission schedule for submitting SSPs was unrealistic in light of the tasks involved. The commenter also thought that, if DHS found fault with a provision of the SVA, it would be unreasonable to begin development of an SSP based upon a potentially flawed assessment. Consequently, the commenter argued that the submission time of 120 days should be started only after the Department's approval of the SVA is formally received. Yet another commenter believed that submission of SSPs should be timed according to the tier assigned to the facility and that the time clock should begin when the facility receives word back from the Department on its preliminary tier assignment.

Response: The Department has established a schedule for activities under this part that considers the need to generally address the risks associated with higher tier facilities before that of lower tiers, but staggers the submittals and review and inspection activities. The Department has developed the Chemical Security Assessment Tool (CSAT) to assist chemical facilities with all of the program requirements (registration, screening, SVA, and SSP). In addition, because information from the CSAT applications will be in electronic form, DHS will be able to expedite its review of the information that chemical facilities submit. These deadlines are both prudent and achievable. DHS expects that it will complete its review of the Top-Screen, SVA, and SSP within 60 days of the facility's submission of the Top-Screen, SVA, or SSP.

6. Alternate Security Programs

Comment: The use of alternate security programs was supported by several chemical companies and associations as well as companies and associations in related industries. A chemical company agreed with the concept of initially allowing multiple methodologies and then switching to a common methodology for at least the Tier 1 facilities; they encouraged DHS to still allow alternate approaches for other tiers. This viewpoint was echoed by at least one association. Several companies wanted to ensure that existing plans could be used and one association noted that more methodologies than just those approved by the Center for Chemical Process Safety (CCPS) would be appropriate. Commenters also noted that CCPS should not be the sole arbiter unless DHS periodically reviews its resources and expertise.

A number of industry associations offered their own approaches and a food industry association commented on the need to keep their current programs in place and to not unduly focus on ammonia refrigeration risks. MTSA-, Sandia-, and NFPA-approved programs were among those mentioned by the commenters, as were those allowed under other regulations. Some commenters found the specific process for approval of alternative programs to be lacking in detail. One association requested that submitters just send in a form saying they have an alternate security plan, and not require any other document be submitted for approval.

An advocacy group commented that alternate approaches needed to be equivalent to the DHS approach, not just sufficiently similar, and that DHS should approve equivalent State and local programs. Another advocacy group suggested that DHS should only determine equivalency based on reviews of individual SSPs, not in any blanket or broad way. A third advocacy group supported a single, consistent approach set out by DHS with private sector programs being modified to conform to the DHS approach. One commenter noted that the specification of RAMCAP may have created an unfair playing field for other firms wanting to visit the source company for RAMCAP.

Response: The Assistant Secretary will review and may approve an ASP upon a determination that it meets the requirements of this regulation and provides an equivalent level of security to the level of security established by this part. In its ASP submission, a facility will have to provide sufficient information about the proposed ASP to ensure that the Department can adequately perform a review and make an equivalency determination.

As described below, certain facilities may submit an ASP in lieu of an SVA, an ASP in lieu of a SSP, or both. Accordingly, the ASP option will only be available following the facility's submission, and Department's review, of the Top-Screen. An ASP for an SVA will need to satisfy the requirements provided in § 27.215, and an ASP for an SSP will need to satisfy the requirements provided in § 27.225. The ASP for the SSP will need to describe specific security measures, or metrics for measures, that will allow the ASP to be considered equivalent to an individually-developed SSP, and facilities implementing an ASP will be subject to DHS inspection against the terms of the ASP.

At this time, the Department will only permit Tier 4 facilities (found to be Tier 4 facilities following the Department's preliminary tiering decision pursuant to § 27.220(a)) to submit an ASP in lieu of an SVA. Tier 4 facilities may submit for review and approval the Sandia RAM for chemical facilities, the CCPS Methodology for fixed chemical facilities, or any methodology certified by CCPS as equivalent to CCPS and has equivalent steps, assumptions, and outputs and sufficiently addresses the risk-based performance standards and CSAT SVA potential terrorist attack scenarios. The Department is requiring Tier 1, Tier 2, and Tier 3 chemical facilities to use the CSAT SVA methodology for preliminary and final tiering. As discussed above in the summary of changes to Rule Provisions, this will provide a common platform for the analysis of vulnerabilities and will ensure that the Department has a consistent measure of risk across the industry. With respect to SSPs, the Department will permit facilities of all tiers to submit ASPs to satisfy the requirements of this rule.

The Department modified § 27.235 to reflect these requirements. The Department also amended the regulation to link the review and approval procedures for ASPs to the review and approval procedures for SVAs and SSPs.

D. Risk-Based Performance Standards

In the Advance Notice, DHS sought comment on the use of risk-based performance standards to address facility-identified vulnerabilities. The Advance Notice proposed that DHS require covered facilities to select, develop, and implement security measures to satisfy the risk-based performance standards in § 27.230. The measures sufficient to meet these standards would vary depending on the covered facility's risk-based tier. Facilities would address the performance standards in the facility's Site Security Plan, and DHS would verify and validate the facility's implementation of the Site Security Plan during an on-site inspection.

1. General Approach to Performance Standards

Comment: The majority of the commenters supported the proposed regulatory approach due to the flexibility that the risk-based performance standards provide to the regulated community in choosing security measures for their respective facilities. The proposed approach acknowledges the fact that each of the facilities faces different security challenges. A few commenters noted

that the goal of the performance standards should be to reduce vulnerabilities identified in the SVA, not necessarily reduce all potential consequences or mandate the use of specific countermeasures.

By contrast, some other commenters opposed the Department's proposed regulatory approach, noting various reasons: that the Advance Notice was too prescriptive in certain areas; that performance standards are open to interpretation and thus can become discretionary, interpretive, and sometimes arbitrary; that chemical companies may be allowed under the rule to make risk reduction determinations based on their available risk reduction budget, rather than on the actual elimination or reduction of the most serious risks; that the rule allows enormous flexibility and variability in the documents that facilities can submit to the Department, which could make program review difficult and hinder any comparative analysis of risk reduction efforts among similar sites.

Response: The Department's statutory authority mandates the issuance of performance standards. Section 550 requires the Department to issue interim final regulations "establishing risk-based performance standards for security chemical facilities." *See* § 550(a). Also, as noted in the Advance Notice, Executive Order 12866 also directs federal agencies to use performance standards. *See* 71 FR 78276, 78283. Performance standards avoid prescriptive requirements, and although they provide flexibility, they still establish and maintain a non-arbitrary threshold standard that facilities will have to reach in order to gain DHS approval under the regulation. The ultimate purpose of the performance standards is to reduce vulnerabilities, and that is regardless of risk reduction budgets.

With respect to documentation, except as provided in § 27.235 for Alternative Security Programs, DHS is requiring facilities to electronically submit all documentation required for analysis and approval. Facilities will complete the Top-Screen, Security Vulnerability Assessment, and Site Security Plans through the online, Web-based CSAT system. This electronic submission will minimize the variability concerns and allow DHS to manage and protect information.

Comment: Regarding the application of the performance standards, some commenters thought that facilities should not have to address all performance standards (listed in § 27.230) in their Site Security Plan and should only have to address those performance standards that directly apply to its facility and its risk-based tier. One commenter thought that, in certain circumstances, a covered facility should be able provide adequate chemical security without implementing every one of the risk-based performance standards. The commenter stated that the regulations should allow for situations where the facility can demonstrate that, under its particular circumstances, one or more of the risk-based performance standards is unnecessary or redundant.

Response: Congress intended for the performance standards to provide facilities with a degree of flexibility in the selection of security measures, and the Department has tried to provide that flexibility throughout the rule. DHS expects that a facility will need to address only those performance standards that apply directly to their facility. In addition, DHS notes that there may be circumstances in which a facility needs not implement one or more of the risk-based performance standards and will still be able to provide adequate chemical security; the Department will work with these facilities on a case-by-case basis in these specific situations.

Comment: Several commenters stated that the proposed standards do not include clear security goals, outcomes, or results to measure increased security. They also asserted that DHS should develop a measurement of vulnerability or risk reduction. One commenter suggested that chemical facilities should identify operational and protection goals and that the protection system should be evaluated with respect to meeting these goals. Another commenter suggested that DHS express the performance standards in terms of overall vulnerability scores as measures via a common Security Vulnerability Assessment methodology. This alternative would allow facilities to devote their security expenses to those measures that would produce the greatest vulnerability reductions and would result, nationally, in the greatest amount of overall vulnerability reduction per dollar spent.

Response: DHS intends for the risk-based performance standards to provide facility owners with the flexibility to choose security measures in their Site Security Plan that will reduce the facility's level of risk. The Security Vulnerability Assessment process, and DHS's resulting placement of the facility within the tier structure, will provide facility owner-operators with an indication of their level of risk.

Comment: Many commenters supported DHS's intention to issue guidance to assist the regulated community in the interpretation and application of the proposed performance standards. They encouraged the Department to work with the regulated community on the development of such guidance. However, some of these same commenters also emphasized that, to effectuate Congress' intention that the chemical security requirements be risk-based performance standards rather than prescriptive requirements, DHS must explicitly make the guidance non-binding. Consistent with the comments about CVI, one commenter discussed the importance of limiting public access to the completed guidance since it could serve as a roadmap for terrorists.

Response: DHS intends to release non-binding guidance on the application of the performance standards in § 27.230 to the risk-based tiers of covered facilities. This guidance will contain sensitive information concerning anti-terrorism measures, and DHS will make that guidance available to those individuals and entities with an appropriate need for the document. DHS will provide the guidance to the House of Representatives Committee on Homeland Security and the Senate Committee on Homeland Security and Governmental Affairs.

2. Comments About Specific Performance Standards

Comment: Several commenters requested clarification about the performance standards in proposed § 27.230(a). A few asked whether paragraph (a)(5) is intended to cover all Department of Transportation hazardous materials and whether it is intended to cover transportation and storage of hazardous materials. One suggested that paragraph (a)(5) should include a provision for securing and monitoring the storage of hazardous materials, in addition to securing and monitoring the shipping and receipt of hazardous materials. Commenters also requested that DHS have facilities report significant security incidents to local law enforcement in addition to the Department. Another commenter indicated that the Department should require the following additional elements in the performance standards: written job descriptions for security personnel, adequate response teams and resources, safe shutdown procedures, evacuation procedures, and decontamination facilities. In addition, another commenter asked that DHS define "dangerous substances and devices" as used in § 27.230(a)(3)(i), "potentially dangerous chemicals" as used in § 27.230(a)(6), and "significant

security incidents" and "suspicious activities" as used in §§ 27.230(a)(15) and 27.230(a)(16). Another commenter asked to whom facilities should report "significant security incidents."

Response: These comments relate to the measures that facilities must select, develop, and implement in their Site Security Plans. The Department will provide information in guidance to facilities on these measures. That might include information on the meaning of these terms, details on the parties to whom facilities should report security incidents and suspicious activities, and explanations about the role of local law enforcement (e.g., the Department's recognition that some investigations of potentially illegal conduct may be the role of local law enforcement).

In addition, DHS also notes that it has made a few changes to the regulatory context based on these comments. As discussed in the summary of regulatory text changes, the Department has revised paragraphs (a)(5), (8), (12), and (15).

Comment: Several comments discussed the need for approaches that address cyber security risks, with several asserting that it is not sufficient for DHS to consider security only from a physical perspective. Commenters opined that there were very few specific references to cyber security in the Advance Notice, even though it is important. Some commenters suggested that DHS should address cyber security in more detail in its own performance standard (i.e., a performance standard that only addresses cyber security), while others suggested that DHS should integrate cyber considerations into other performance standards. Other commenters asked DHS to identify the scope of "cyber" security and "other sensitive computerized systems" in paragraph (a)(8).

Commenters also raised other issues related to cyber security. One commenter mentioned that cyber or joint physical/cyber intrusions could create dangerous chemicals that did not previously exist. Consequently, commenters thought that DHS should address these contingencies in the screening process and/or issue an expansive list of chemicals. Other commenters noted that the RAMCAP approach was not designed to address control system cyber security. A few other commenters believed that the tiering approach is not appropriate for cyber security of control systems. Additionally, commenters mentioned that it is important to consider that facilities with interconnecting electronic systems could face additional threats as one site's vulnerability poses a risk to other connected sites.

Response: The Department recognizes that cyber security is an issue and has included cyber security as one of the performance standards that facilities must address in their Site Security Plans. Paragraph (c)(8) requires facilities to select, develop, and implement measures that "deter cyber sabotage." In addition, the Department notes that it has implemented an assessment of cyber vulnerabilities for industrial control systems within the CSAT Security Vulnerability Assessment. The Department has accomplished this through the assistance of DHS's National Cyber Security Division (NCSD). DHS appreciates the complexity and uniqueness of addressing cyber security with chemical facilities and anticipates that the CSAT will mature over time, especially with the constructive feedback from interested and knowledgeable parties.

Comment: The Department received numerous comments on its use of the acronym "SCADA" in § 27.230(a)(8). Commenters asserted that SCADA refers to a central control system that monitors and controls a complete site or a system spread out over a long distance. They noted that using the term SCADA to represent cyber systems at chemical facilities is too narrow and suggested that the Department should replace the term SCADA with "Industrial Control Systems."

Response: While the Department had used the acronym "SCADA" (Supervisory Control and Data Acquisition) in the Advance Notice as shorthand for instrumented control systems in general, the Department agrees with the comments and has incorporated broader, more descriptive terminology into this performance standard. The Department has revised § 27.230(a)(8), so that it reads as follows: "Each covered facility must select, develop, and implement measures designed to: * * * [d]eter cyber sabotage, including by preventing unauthorized onsite or remote access to critical process controls, such as Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), Industrial Control Systems (ICS), critical business systems, and other sensitive computerized systems."

3. Variations in Performance Standards for Risk Tiers

Comment: Several commenters supported the use of risk-based tiers, with several recommending that DHS consult with industry in the development of specific performance standards for each tier. Various commenters favored the Department's proposal to place high-risk facilities in risk-based tiers and to prioritize the implementation phase-in and the level of regulatory scrutiny (i.e., frequency of regulatory reviews, inspections and SVA/SSP updates) based on the facility's risk and associated tier. Commenters noted that DHS should require facilities in higher risk tiers to develop more robust measures to meet the performance standards.

In contrast, a few other commenters had differing opinions. A small number of comments cautioned that performance standards should be consistent across all tiers, regardless of the level of risk. These commenters noted that DHS should adjust the specific measures, not the performance standards, to match the level of risk. In addition, one commenter stated that DHS should not establish risk-based tiers and should instead identify the criteria for those facilities that will be regulated and those that will not. If DHS were to establish tiers, that commenter thought DHS should limit the tiers to high or low risk.

Response: As discussed above in Section III(B)(3), DHS is creating four risk-based tiers, with the highest risk facilities in the top tier (i.e., Tier 1). The types and intensity of security measures (sufficient to satisfy the risk-based performance standards in the facility's Site Security Plan) will depend on the facility's tier. For facilities that present the greatest degree of risk, more rigorous security measures will be needed to satisfy the performance standards. The Department will use a higher level of regulatory scrutiny for facilities that present the highest risk.

DHS consulted with the chemical industry in developing the tier system and performance standards. In adopting the four tier system and applicable risk-based performance standards, DHS intends to employ a scalable performance standard across the tiers, i.e., within the same performance standard, a more robust set of security measures will be needed for a Tier 1 facility than for a Tier 2 facility, for a Tier 2 facility than for a Tier 3 facility, and so on. DHS will ensure that risk-based performance standards are applied consistently across each tier, but guidelines for each tier will vary.

Comment: A few commenters also supported the idea that a facility, which the Department has previously determined is "high risk," can request that the Department move it to a lower tier if it has materially altered its operations in a way that significantly

Bill Analysis

Gerald T. Noel, Jr. *Legislative Service Commission*

S.B. 258

124th General Assembly
(As Introduced)

Sens. Austria, Goodman, Randy Gardner

BILL SUMMARY

- Requires the fire chief of a township, fire district, city fire department, or village fire department to request the Superintendent of the Bureau of Criminal Identification and Investigation (BCII) to conduct a criminal records check with respect to any person who is under final consideration for appointment or employment as a full-time paid firefighter.
- Permits the fire chief of a township, fire district, city fire department, or village fire department to request the Superintendent of BCII to conduct a criminal records check with respect to any person who is under final consideration for appointment as a volunteer firefighter.
- Exempts from the Public Records Law specified residential and familial information of a member of a fire department.
- Provides that a record kept by a public office that is a "security record" or "infrastructure record" is not a public record under the Public Records Law and is not subject to mandatory release or disclosure under that Law.

CONTENT AND OPERATION

Criminal records checks

Required for full-time paid firefighters; permissible for volunteer firefighters

The bill requires the fire chief of a township, fire district, city fire department, or village fire department (hereafter fire chief refers to a fire chief of all of the four entities) to request the Superintendent of the Bureau of Criminal Identification and Investigation (BCII) to conduct a criminal records check with respect to any person who is under final consideration for appointment or

employment as a full-time paid firefighter. The bill permits the fire chief to request the Superintendent of BCII to conduct a criminal records check with respect to any person who is under final consideration for appointment as a volunteer firefighter.

The bill requires a fire chief who requests a criminal records check to inform each person who is the applicant, at the time of the person's initial application for appointment or employment that the person subject to the criminal records check is required to provide a set of impressions of the person's fingerprints and that a criminal records check is required to be conducted and satisfactorily completed. (R.C. 505.381(A) and (G), 737.081(A) and (G), and 737.221(A) and (G).)

Upon receipt of a request for a criminal records check under the bill, the completed information form, and a set of fingerprint impressions, the Superintendent of BCII must conduct a criminal records check to determine if any information exists that indicates that the person subject to the request has been convicted of or pleaded guilty to any disqualifying offense (see "***Appointment***," below). The Superintendent must review all records gathered by BCII, any relevant sealed information, and, upon request, any Federal Bureau of Investigation (FBI) provided information. The Superintendent must respond within 90 days after receipt of the request (R.C. 109.572(A)(6), (A)(9), and (B)).

Procedure

The bill provides that if a person subject to a criminal records check does not present proof that the person has been a resident of this state for the five-year period immediately prior to the date upon which the criminal records check is requested or does not provide evidence that within that five-year period the Superintendent of BCII has requested information about the person from the FBI in a criminal records check, the fire chief may request that the Superintendent of BCII obtain information from the FBI as a part of the criminal records check. If the person subject to the criminal records check presents proof that the person has been a resident of this state for that five-year period, the fire chief may request that the Superintendent of BCII include information from the FBI in the criminal records check. The fire chief, therefore, may request FBI information whether or not the person has been a resident for the five-year period or FBI information has been provided during that five-year period.

The bill also provides that a fire chief required to request a criminal records check must provide to each person who is subject to a criminal records check a copy of the information form and standard fingerprint impression sheet prescribed under current law, obtain the completed information form and impression sheet from the person, and forward the completed information form and impression

sheet to the Superintendent of BCII at the time the criminal records check is requested.

The bill further provides that any person who is subject to a criminal records check, who receives a copy of the information form and a copy of the fingerprint impression sheet, and who is requested to complete the information form and provide a set of fingerprint impressions must complete the information form or provide all the information necessary to complete the information form and must provide the impression sheet with the impressions of the person's fingerprints. If the person fails to provide the information necessary to complete the form or fails to provide impressions of the person's fingerprints, the appointing authority is prohibited from appointing or employing the person as a permanent full-time paid firefighter or a volunteer firefighter. (R.C. 505.381(B), 737.081(B), and 737.221(B).)

Appointment

The bill prohibits an appointing authority from appointing or employing a person as a permanent full-time paid firefighter or a volunteer firefighter if the person previously has been convicted of or pleaded guilty to any of the following: (a) a felony, (b) arson, or (c) a violation of an existing or former law of this state, any other state, or the United States that is substantially equivalent to a felony or arson.

The bill permits an appointing authority to appoint or employ a person as a permanent full-time paid firefighter or volunteer firefighter conditionally until the criminal records check is completed and the fire chief receives the results of the criminal records check. If the results of the criminal records check indicate that the person does not qualify for appointment or employment, the fire chief must release the person from appointment or employment. (R.C. 505.381(C), 737.081(C), and 737.221(C).)

Miscellaneous provisions relating to the criminal records check

The bill requires the fire chief to pay to BCII the fee required under current law for each criminal records check conducted in accordance with the current law upon a request under the bill. The bill permits the fire chief to charge the person subject to the criminal records check a fee for the costs the fire chief incurs in obtaining the criminal records check. The fee charged cannot exceed the amount of fees the fire chief pays for the criminal records check. If a fee is charged to the person subject to the criminal records check, the fire chief must notify the person who is the applicant at the time of the person's initial application for appointment or employment of the amount of the fee and that, unless the fee is paid, the person

will not be considered for appointment or employment. (R.C. 505.381(D), 737.081(D), and 737.221(D).)

The bill exempts from the Public Records Law the report of any criminal records check conducted by BCII pursuant to a request made under the bill. The report may not be made available to any person other than the person who is the subject of the criminal records check or the person's representative or the fire chief requesting the criminal records check or the fire chief's representative. (R.C. 505.381(E), 737.081(E), and 737.221(E).)

The bill requires the appointing authority to adopt rules in accordance with the Administrative Procedure Act to implement the provisions of the bill. The rules must include rehabilitation standards a person who has been convicted of or pleaded guilty to a felony, arson, or an equivalent offense must meet for the appointing authority to appoint or employ the person as a permanent full-time paid firefighter or a volunteer firefighter (R.C. 505.381(F), 737.081(F), and 737.221(F)).

The bill defines "appointing authority" as any person or body that has the authority to hire, appoint, or employ permanent, full-time paid firefighters and volunteer firefighters (R.C. 505.381(H)(1), 737.081(H)(1), and 737.221(H)(1)).

Public Records Law

Existing law

In general. The existing Public Records Law (R.C. 149.43) specifies that, generally, all "public records" (see below) must be promptly prepared and made available for inspection to any person at all reasonable times during regular business hours. Upon request, a public office or person responsible for public records generally must make copies available at cost, within a reasonable period of time. (R.C. 149.43(B).)

Public record. For purposes of the Public Records Law, "public record" generally means any "record" (see below) that is kept by any "public office" (see below), including, but not limited to, state, county, city, village, township, and school district units. But, "public record" does not mean any of the following: (1) medical records, (2) records pertaining to probation and parole proceedings, (3) records pertaining to certain abortion-related actions and to appeals of those actions, (4) records pertaining to adoption proceedings, including the contents of an adoption file maintained by the Department of Health, (5) information in a record contained in the Putative Father Registry, (6) certain adoption-related records, (7) trial preparation records, (8) confidential law enforcement investigatory records, (9) certain mediation and civil rights action records, (10)

DNA records stored in BCII's DNA Database, (11) inmate records released by the Department of Rehabilitation and Correction to the Department of Youth Services or a court of record, (12) records maintained by the Department of Youth Services pertaining to children in its custody released by it to the Department of Rehabilitation and Correction, (13) intellectual property records, (14) donor profile records, (15) records maintained by the Department of Job and Family Services in its New Hires Directory, (16) peace officer residential and familial information, (17) in the case of a county hospital, information that constitutes a trade secret, (18) information pertaining to the recreational activities of a person under the age of 18, (19) generally, records provided to, statements made by review board members during meetings of, and all work products of a child fatality review board, (20) certain records provided to and statements made by the executive director of a public children services agency or a prosecuting attorney pertaining to the death of a child, (21) test materials, examinations, or evaluation tools used in an examination for licensure as a nursing home administrator that the board of examiners of nursing home administrators administers or contracts under that section with a private or government entity to administer, or (22) records the release of which is prohibited by state or federal law. (R.C. 149.43(A)(1).)

The Law also defines "confidential law enforcement investigatory record," "medical record," "trial preparation record," "intellectual property record," "donor profile record," "peace officer residential and familial information" (see **COMMENT** 1), and "information pertaining to the recreational activities of a person under the age of 18 (R.C. 149.43(A)(2) to (8)).

Public office; record. Existing R.C. 149.011, not in the bill, defines certain terms for use throughout R.C. Chapter 149., as follows (R.C. 149.011):

(1) "Public office" includes any state agency, public institution, political subdivision, or any other organized body, office, agency, institution, or entity established by the laws of this state for the exercise of any function of government. As used in this definition, "state agency" includes every department, bureau, board, commission, office, or other organized body established by the Constitution and laws of Ohio for the exercise of any function of state government, including any state-supported institution of higher education, the General Assembly, or any legislative agency, any court or judicial agency, or any political subdivision or agency thereof.

(2) "Records" includes any document, device, or item, regardless of physical form or characteristic, created or received by or coming under the jurisdiction of any public office of the state or its political subdivisions, which serves to document the organization, functions, policies, decisions, procedures, operations, or other activities of the office.

Operation of the bill

The bill enacts two new, specific exceptions to the Public Records Law.

First, the bill provides that, for purposes of the Public Records Law, "public record" does not include firefighter residential and familial information. (R.C. 149.43(A)(1)(w) (see **COMMENT** 2).)

Second, the bill provides that a record kept by a public office that is a "security record" or "infrastructure record" (see below) is not a public record under the Public Records Law and is not subject to mandatory release or disclosure under that Law.

It also provides that, notwithstanding any other Revised Code section, a public office's or a public employee's disclosure of a security record or infrastructure record that is necessary for construction, renovation, or remodeling work on any public building or project does not constitute public disclosure for purposes of waiving the preceding paragraph and does not result in that record becoming a public record for purposes of the Public Records Law. (R.C. 149.433(B) and (C).)

The bill specifies that, as used in the above provisions, the following terms have the following meanings (R.C. 149.433(A)):

(1) "Act of terrorism" has the same meaning as in R.C. 2909.21 (R.C. 149.433(A)(1) (not in this bill, see **COMMENT** 3)).

(2) "Infrastructure record" means any record that discloses the configuration of a public office's critical systems including, but not be limited to, communication, computer, electrical, mechanical, ventilation, water, and plumbing systems, security codes, or the infrastructure or structural configuration of the building in which a public office is located. "Infrastructure record" does not mean a simple floor plan that discloses only the spatial relationship of components of a public office or the building in which a public office is located. (R.C. 149.433(A)(2).)

(3) "Security record" means either of the following (R.C. 149.433(A)(3)):

(a) Any record that contains information directly used for protecting or maintaining the security of a public office against attack, interference, or sabotage;

(b) Any record assembled, prepared or maintained by a public office or public body to prevent, mitigate, or respond to acts of terrorism, including the following: (i) those portions of records containing specific and unique vulnerability assessments or specific and unique response plans either of which is

intended to prevent or mitigate acts of terrorism, and communication codes or deployment plans of law enforcement or emergency response personnel, (ii) specific intelligence information and specific investigative records shared by federal and international law enforcement agencies with state and local law enforcement and public safety agencies, and (iii) 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.

COMMENT

1. Existing law defines "peace officer residential and familial information" as any information maintained in a personnel record of a peace officer that discloses any of the following: (a) the address of the actual personal residence of a peace officer, except for the state or political subdivision in which the peace officer resides, (b) information compiled from referral to or participation in an employee assistance program, (c) the social security number, the residential telephone number, any bank account, debit card, charge card, or credit card number, or the emergency telephone number of, or any medical information pertaining to, a peace officer, (d) the name of any beneficiary of employment benefits, including, but not limited to, life insurance benefits, provided to a peace officer by the peace officer's employer, (e) the identity and amount of any charitable or employment benefit deduction made by the peace officer's employer from the peace officer's compensation unless the amount of the deduction is required by state or federal law, and (f) the name, the residential address, the name of the employer, the address of the employer, the social security number, the residential telephone number, any bank account, debit card, charge card, or credit card number, or the emergency telephone number of the spouse, a former spouse, or any child of a peace officer.

Existing law also defines "peace officer residential and familial information" as any record that identifies a person's occupation as a peace officer other than statements required to include the disclosure of that fact under the campaign finance law. (R.C. 149.43(A)(7).)

2. The bill does not define "firefighter residential and familial information" in a manner similar to the definition of "peace officer residential and familial information" under existing law or in any other manner.

3. Am. Sub. S.B. 184, signed by the Governor on May 15, 2002, enacts a definition of "act of terrorism," which means an act that is committed within or outside the territorial jurisdiction of this state or the United States, that constitutes

a specified offense if committed in this state or constitutes an offense in any jurisdiction within or outside the territorial jurisdiction of the United States containing all of the essential elements of a specified offense, and that is intended to do one or more of the following: (1) intimidate or coerce a civilian population, (2) influence the policy of any government by intimidation or coercion, or (3) affect the conduct of any government by the act that constitutes the offense (R.C. 2909.21(A)).

HISTORY

ACTION	DATE	JOURNAL ENTRY
Introduced	04-23-02	p. 1690

s0258-i.124/kl

Gerald T. Noel, Jr. *Legislative Service Commission*

S.B. 258

124th General Assembly
(As Introduced)

Sens. Austria, Goodman, Randy Gardner

BILL SUMMARY

- Requires the fire chief of a township, fire district, city fire department, or village fire department to request the Superintendent of the Bureau of Criminal Identification and Investigation (BCII) to conduct a criminal records check with respect to any person who is under final consideration for appointment or employment as a full-time paid firefighter.
- Permits the fire chief of a township, fire district, city fire department, or village fire department to request the Superintendent of BCII to conduct a criminal records check with respect to any person who is under final consideration for appointment as a volunteer firefighter.
- Exempts from the Public Records Law specified residential and familial information of a member of a fire department.
- Provides that a record kept by a public office that is a "security record" or "infrastructure record" is not a public record under the Public Records Law and is not subject to mandatory release or disclosure under that Law.

CONTENT AND OPERATION

Criminal records checks

Required for full-time paid firefighters; permissible for volunteer firefighters

The bill requires the fire chief of a township, fire district, city fire department, or village fire department (hereafter fire chief refers to a fire chief of all of the four entities) to request the Superintendent of the Bureau of Criminal Identification and Investigation (BCII) to conduct a criminal records check with respect to any person who is under final consideration for appointment or

employment as a full-time paid firefighter. The bill permits the fire chief to request the Superintendent of BCII to conduct a criminal records check with respect to any person who is under final consideration for appointment as a volunteer firefighter.

The bill requires a fire chief who requests a criminal records check to inform each person who is the applicant, at the time of the person's initial application for appointment or employment that the person subject to the criminal records check is required to provide a set of impressions of the person's fingerprints and that a criminal records check is required to be conducted and satisfactorily completed. (R.C. 505.381(A) and (G), 737.081(A) and (G), and 737.221(A) and (G).)

Upon receipt of a request for a criminal records check under the bill, the completed information form, and a set of fingerprint impressions, the Superintendent of BCII must conduct a criminal records check to determine if any information exists that indicates that the person subject to the request has been convicted of or pleaded guilty to any disqualifying offense (see "***Appointment***," below). The Superintendent must review all records gathered by BCII, any relevant sealed information, and, upon request, any Federal Bureau of Investigation (FBI) provided information. The Superintendent must respond within 90 days after receipt of the request (R.C. 109.572(A)(6), (A)(9), and (B)).

Procedure

The bill provides that if a person subject to a criminal records check does not present proof that the person has been a resident of this state for the five-year period immediately prior to the date upon which the criminal records check is requested or does not provide evidence that within that five-year period the Superintendent of BCII has requested information about the person from the FBI in a criminal records check, the fire chief may request that the Superintendent of BCII obtain information from the FBI as a part of the criminal records check. If the person subject to the criminal records check presents proof that the person has been a resident of this state for that five-year period, the fire chief may request that the Superintendent of BCII include information from the FBI in the criminal records check. The fire chief, therefore, may request FBI information whether or not the person has been a resident for the five-year period or FBI information has been provided during that five-year period.

The bill also provides that a fire chief required to request a criminal records check must provide to each person who is subject to a criminal records check a copy of the information form and standard fingerprint impression sheet prescribed under current law, obtain the completed information form and impression sheet from the person, and forward the completed information form and impression

sheet to the Superintendent of BCII at the time the criminal records check is requested.

The bill further provides that any person who is subject to a criminal records check, who receives a copy of the information form and a copy of the fingerprint impression sheet, and who is requested to complete the information form and provide a set of fingerprint impressions must complete the information form or provide all the information necessary to complete the information form and must provide the impression sheet with the impressions of the person's fingerprints. If the person fails to provide the information necessary to complete the form or fails to provide impressions of the person's fingerprints, the appointing authority is prohibited from appointing or employing the person as a permanent full-time paid firefighter or a volunteer firefighter. (R.C. 505.381(B), 737.081(B), and 737.221(B).)

Appointment

The bill prohibits an appointing authority from appointing or employing a person as a permanent full-time paid firefighter or a volunteer firefighter if the person previously has been convicted of or pleaded guilty to any of the following: (a) a felony, (b) arson, or (c) a violation of an existing or former law of this state, any other state, or the United States that is substantially equivalent to a felony or arson.

The bill permits an appointing authority to appoint or employ a person as a permanent full-time paid firefighter or volunteer firefighter conditionally until the criminal records check is completed and the fire chief receives the results of the criminal records check. If the results of the criminal records check indicate that the person does not qualify for appointment or employment, the fire chief must release the person from appointment or employment. (R.C. 505.381(C), 737.081(C), and 737.221(C).)

Miscellaneous provisions relating to the criminal records check

The bill requires the fire chief to pay to BCII the fee required under current law for each criminal records check conducted in accordance with the current law upon a request under the bill. The bill permits the fire chief to charge the person subject to the criminal records check a fee for the costs the fire chief incurs in obtaining the criminal records check. The fee charged cannot exceed the amount of fees the fire chief pays for the criminal records check. If a fee is charged to the person subject to the criminal records check, the fire chief must notify the person who is the applicant at the time of the person's initial application for appointment or employment of the amount of the fee and that, unless the fee is paid, the person

will not be considered for appointment or employment. (R.C. 505.381(D), 737.081(D), and 737.221(D).)

The bill exempts from the Public Records Law the report of any criminal records check conducted by BCII pursuant to a request made under the bill. The report may not be made available to any person other than the person who is the subject of the criminal records check or the person's representative or the fire chief requesting the criminal records check or the fire chief's representative. (R.C. 505.381(E), 737.081(E), and 737.221(E).)

The bill requires the appointing authority to adopt rules in accordance with the Administrative Procedure Act to implement the provisions of the bill. The rules must include rehabilitation standards a person who has been convicted of or pleaded guilty to a felony, arson, or an equivalent offense must meet for the appointing authority to appoint or employ the person as a permanent full-time paid firefighter or a volunteer firefighter (R.C. 505.381(F), 737.081(F), and 737.221(F)).

The bill defines "appointing authority" as any person or body that has the authority to hire, appoint, or employ permanent, full-time paid firefighters and volunteer firefighters (R.C. 505.381(H)(1), 737.081(H)(1), and 737.221(H)(1)).

Public Records Law

Existing law

In general. The existing Public Records Law (R.C. 149.43) specifies that, generally, all "public records" (see below) must be promptly prepared and made available for inspection to any person at all reasonable times during regular business hours. Upon request, a public office or person responsible for public records generally must make copies available at cost, within a reasonable period of time. (R.C. 149.43(B).)

Public record. For purposes of the Public Records Law, "public record" generally means any "record" (see below) that is kept by any "public office" (see below), including, but not limited to, state, county, city, village, township, and school district units. But, "public record" does not mean any of the following: (1) medical records, (2) records pertaining to probation and parole proceedings, (3) records pertaining to certain abortion-related actions and to appeals of those actions, (4) records pertaining to adoption proceedings, including the contents of an adoption file maintained by the Department of Health, (5) information in a record contained in the Putative Father Registry, (6) certain adoption-related records, (7) trial preparation records, (8) confidential law enforcement investigatory records, (9) certain mediation and civil rights action records, (10)

DNA records stored in BCII's DNA Database, (11) inmate records released by the Department of Rehabilitation and Correction to the Department of Youth Services or a court of record, (12) records maintained by the Department of Youth Services pertaining to children in its custody released by it to the Department of Rehabilitation and Correction, (13) intellectual property records, (14) donor profile records, (15) records maintained by the Department of Job and Family Services in its New Hires Directory, (16) peace officer residential and familial information, (17) in the case of a county hospital, information that constitutes a trade secret, (18) information pertaining to the recreational activities of a person under the age of 18, (19) generally, records provided to, statements made by review board members during meetings of, and all work products of a child fatality review board, (20) certain records provided to and statements made by the executive director of a public children services agency or a prosecuting attorney pertaining to the death of a child, (21) test materials, examinations, or evaluation tools used in an examination for licensure as a nursing home administrator that the board of examiners of nursing home administrators administers or contracts under that section with a private or government entity to administer, or (22) records the release of which is prohibited by state or federal law. (R.C. 149.43(A)(1).)

The Law also defines "confidential law enforcement investigatory record," "medical record," "trial preparation record," "intellectual property record," "donor profile record," "peace officer residential and familial information" (see **COMMENT** 1), and "information pertaining to the recreational activities of a person under the age of 18 (R.C. 149.43(A)(2) to (8)).

Public office; record. Existing R.C. 149.011, not in the bill, defines certain terms for use throughout R.C. Chapter 149., as follows (R.C. 149.011):

(1) "Public office" includes any state agency, public institution, political subdivision, or any other organized body, office, agency, institution, or entity established by the laws of this state for the exercise of any function of government. As used in this definition, "state agency" includes every department, bureau, board, commission, office, or other organized body established by the Constitution and laws of Ohio for the exercise of any function of state government, including any state-supported institution of higher education, the General Assembly, or any legislative agency, any court or judicial agency, or any political subdivision or agency thereof.

(2) "Records" includes any document, device, or item, regardless of physical form or characteristic, created or received by or coming under the jurisdiction of any public office of the state or its political subdivisions, which serves to document the organization, functions, policies, decisions, procedures, operations, or other activities of the office.

Operation of the bill

The bill enacts two new, specific exceptions to the Public Records Law.

First, the bill provides that, for purposes of the Public Records Law, "public record" does not include firefighter residential and familial information. (R.C. 149.43(A)(1)(w) (see **COMMENT** 2).)

Second, the bill provides that a record kept by a public office that is a "security record" or "infrastructure record" (see below) is not a public record under the Public Records Law and is not subject to mandatory release or disclosure under that Law.

It also provides that, notwithstanding any other Revised Code section, a public office's or a public employee's disclosure of a security record or infrastructure record that is necessary for construction, renovation, or remodeling work on any public building or project does not constitute public disclosure for purposes of waiving the preceding paragraph and does not result in that record becoming a public record for purposes of the Public Records Law. (R.C. 149.433(B) and (C).)

The bill specifies that, as used in the above provisions, the following terms have the following meanings (R.C. 149.433(A)):

(1) "Act of terrorism" has the same meaning as in R.C. 2909.21 (R.C. 149.433(A)(1) (not in this bill, see **COMMENT** 3)).

(2) "Infrastructure record" means any record that discloses the configuration of a public office's critical systems including, but not be limited to, communication, computer, electrical, mechanical, ventilation, water, and plumbing systems, security codes, or the infrastructure or structural configuration of the building in which a public office is located. "Infrastructure record" does not mean a simple floor plan that discloses only the spatial relationship of components of a public office or the building in which a public office is located. (R.C. 149.433(A)(2).)

(3) "Security record" means either of the following (R.C. 149.433(A)(3)):

(a) Any record that contains information directly used for protecting or maintaining the security of a public office against attack, interference, or sabotage;

(b) Any record assembled, prepared or maintained by a public office or public body to prevent, mitigate, or respond to acts of terrorism, including the following: (i) those portions of records containing specific and unique vulnerability assessments or specific and unique response plans either of which is

intended to prevent or mitigate acts of terrorism, and communication codes or deployment plans of law enforcement or emergency response personnel, (ii) specific intelligence information and specific investigative records shared by federal and international law enforcement agencies with state and local law enforcement and public safety agencies, and (iii) 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.

COMMENT

1. Existing law defines "peace officer residential and familial information" as any information maintained in a personnel record of a peace officer that discloses any of the following: (a) the address of the actual personal residence of a peace officer, except for the state or political subdivision in which the peace officer resides, (b) information compiled from referral to or participation in an employee assistance program, (c) the social security number, the residential telephone number, any bank account, debit card, charge card, or credit card number, or the emergency telephone number of, or any medical information pertaining to, a peace officer, (d) the name of any beneficiary of employment benefits, including, but not limited to, life insurance benefits, provided to a peace officer by the peace officer's employer, (e) the identity and amount of any charitable or employment benefit deduction made by the peace officer's employer from the peace officer's compensation unless the amount of the deduction is required by state or federal law, and (f) the name, the residential address, the name of the employer, the address of the employer, the social security number, the residential telephone number, any bank account, debit card, charge card, or credit card number, or the emergency telephone number of the spouse, a former spouse, or any child of a peace officer.

Existing law also defines "peace officer residential and familial information" as any record that identifies a person's occupation as a peace officer other than statements required to include the disclosure of that fact under the campaign finance law. (R.C. 149.43(A)(7).)

2. The bill does not define "firefighter residential and familial information" in a manner similar to the definition of "peace officer residential and familial information" under existing law or in any other manner.

3. Am. Sub. S.B. 184, signed by the Governor on May 15, 2002, enacts a definition of "act of terrorism," which means an act that is committed within or outside the territorial jurisdiction of this state or the United States, that constitutes

a specified offense if committed in this state or constitutes an offense in any jurisdiction within or outside the territorial jurisdiction of the United States containing all of the essential elements of a specified offense, and that is intended to do one or more of the following: (1) intimidate or coerce a civilian population, (2) influence the policy of any government by intimidation or coercion, or (3) affect the conduct of any government by the act that constitutes the offense (R.C. 2909.21(A)).

HISTORY

ACTION	DATE	JOURNAL ENTRY
Introduced	04-23-02	p. 1690

s0258-i.124/kl

the personally identifiable information contained therein would violate FERPA, which prohibits institutions from releasing a student's "education records" without the written consent of the student or their parents.[362]

Ohio also has a state version of FERPA.[363] Under Ohio law, no person shall release or permit access to any personally identifiable information (except directory information) about a student attending a public school without proper written consent.[364] Accordingly, education officials and employees must be diligent in determining whether to release any record that may identify their students.

7. *Infrastructure & Security Records*

In 2002, the Ohio legislature enacted an anti-terrorism bill. Among other changes to Ohio law, the bill created two new categories of records that are exempt from mandatory public disclosure: "infrastructure records" and "security records."[365]

a. Infrastructure Records

An "infrastructure record" is any record that discloses the configuration of a public office's "critical systems," such as its communications, computer, electrical, mechanical, ventilation, water, plumbing, or security systems.[366] Simple floor plans or records showing the spatial relationship of the public office are not infrastructure records.[367]

The law also states that infrastructure records may be disclosed for purposes of construction, renovation, or remodeling of a public office without waiving the exempt status of that record.[368]

b. Security Records

A "security record" is "any record that contains information directly used for protecting or maintaining the security of a public office against attack, interference, or sabotage or to prevent, mitigate, or respond to acts of terrorism."[369] The law also states that security records may be disclosed for purposes of construction, renovation, or remodeling of a public office without waiving the exempt status of that record.[370]

---

[362] 20 U.S.C. § 1232g(b)(1).
[363] R.C. 3319.321.
[364] R.C. 3319.321(B).
[365] R.C. 149.433.
[366] R.C. 149.433(A)(2).
[367] R.C. 149.433(A)(2).
[368] R.C. 149.433(C).
[369] R.C. 149.433(A)(3)(a),(b).
[370] R.C. 149.433(C).