Kirkpatrick & Lockhart LLP

Homeland Security Issues

By Barry M. Hartman, Craig P. Wilson and Marsha A. Sajer*

I. Homeland Security – An Overview.

See Homeland Security Expands to regulation of the Manufacture, Use, Transportation, and Disposal of Hazardous Substances and Materials, Including Chemical and Biological Agents, HOMELAND SECURITY BULLETIN, by Barry M. Hartman, Christopher E. Dominguez, Marsha A. Sajer, April 2003.

II. Community Water Systems – Vulnerability Assessments.

A. Relevant Statute(s).

Title IV of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Pub. L. 107-188, 116 Stat. 594, 682 (June 12, 2002) ("Bioterrorism Act"), amending the Safe Drinking Water Act (Title XIV of the Public Health Service Act). *See* 42 U.S.C. § 300i-2.

B. Responsible Agency.

Environmental Protection Agency.

C. Regulations.

Not implemented in the Code of Federal Regulations.

---

* *Mr. Hartman is a partner in the Washington office of Kirkpatrick & Lockhart LLP and is the former Acting Assistant Attorney General for the United States Department of Justice Environment and Natural Resources Division. Mr. Wilson is a partner in the Harrisburg, PA office of K&L with a practice concentrated in the areas of environmental compliance counseling and environmental and commercial litigation, including litigation in state and federal courts and before administrative agencies. Ms. Sajer is an associate in the Harrisburg office and previously served as an assistant to the Army General Counsel, where she provided legal advice on a broad range of issues, including disaster and terrorism response.*

D. Agency Guidance.

Instructions to Assist Community Water Systems in Complying with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. *See* EPA 810-B-02-001, January 2003, available at http://www.epa.gov/safewater/security.

E. Summary.

1. Overview.

Title IV of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Pub. L. 107-188, 116 Stat. 594, 682 (June 12, 2002) ("Bioterrorism Act"). The Bioterrorism Act amended the Safe Drinking Water Act by adding section 1433, which directs actions community water systems and the U.S. Environmental Protection Agency ("EPA") must take to improve the security of the nation's drinking water infrastructure.

Section 1433(a) requires certain community water systems to conduct vulnerability assessments, certify to EPA that the vulnerability assessments were conducted, and submit a copy of the vulnerability assessment to the EPA.

Section 1433(b) requires certain community water systems to prepare or revise emergency response plans based on the vulnerability assessment and to certify to EPA that an emergency response plan was completed.

2. Vulnerability assessments.

a. Every CWS[1] serving a population of more than 3,300 persons must conduct a vulnerability assessment of its system to determine its vulnerability to a terrorist attack or other intentional act that would disrupt the system's ability to provide a safe and reliable supply of drinking water. 42 U.S.C § 300i-2(a)(1).

b. The vulnerability assessment must include a review of:

- pipes and constructed conveyances,
- physical barriers,
- water collection, pretreatment, treatment, storage and distribution facilities,

[1] A "community water system" is a public water system that serves at least 15 service connections used by year-round residents of the area served by the system, or regularly serves at least 25 year-round residents. 42 U.S.C. § 300f (15).

- electronic, computer or other automated systems which are utilized by the public water system,
- the use, storage, or handling of various chemicals, and
- the operation and maintenance of such system.

Id.

c. EPA was tasked to provide, by August 1, 2002, information to CWS regarding which kinds of terrorist attacks or other intentional acts are the probable threats to substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water; or otherwise present significant public health concerns. *Id.*

d. The EPA provided an overview of threats, methodologies, and strategies for CWS to consider in developing its vulnerability assessment. *See* Vulnerability Assessment Factsheet available at http://www.epa.gov/safewater/security/va_fact_sheet_12-19.pdf. The EPA also sent a document entitled *Baseline Threat Information for Vulnerability Assessments of Community Water Systems* to each CWS which generally outlines who and what the system should consider as potential threats. This document is treated as sensitive and it not available to the public.

e. Vulnerability assessment steps generally include the following (*see* Appendix 2 to Instructions to Assist Community Water Systems in Complying with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002):

(1) Characterize the water system, including its mission and objectives;

(2) Identify and prioritize adverse consequences to avoid;

(3) Determine critical assets that might be subject to malevolent acts that could result in undesired consequences;

(4) Assess the likelihood of such malevolent acts from adversaries (e.g., terrorists, vandals);

(5) Evaluate existing countermeasures; and

(6) Analyze the current risk and development of a prioritized plan for risk reduction.

3. Certification and submission of vulnerability assessment to EPA.

a. Each CWS serving more than 3,300 persons must certify to EPA that the system conducted a vulnerability assessment and submit a written copy of the assessment to the EPA. *Id.* § 300i-2(a)(2).

b. The date by which a CWS must submit its certified vulnerability assessment to the EPA varies with the size of the system:

- March 31, 2003, for CWS serving a population of 100,000 or more;
- December 31, 2003, for CWS serving a population of 50,000 or more but less than 100,000;
- June 30, 2004, for CWS serving a population greater than 3,300 but less than 50,000.

Id. The EPA will use data filed by the states in the Safe Drinking Water System (SDWIS) to determine the size of a CWS and thus its reporting deadline.

4. Protection of information submitted with vulnerability assessment.

a. Except for the information contained in the certification, all vulnerability assessment information is exempt from disclosure under the Freedom of Information Act (5 U.S.C. § 552). *Id.* § 300i-2(a)(3).

b. No CWS may be required to provide an assessment to any State, regional, or local governmental entity solely by reason of the statutory obligation to provide it to the EPA. *Id.* § 300i-2(a)(4).

c. The law requires the EPA to develop protocols protecting the vulnerability assessments from unauthorized disclosure by November 30, 2002. Each copy of the assessment and related information must be kept in a secure location, and the EPA Administrator would designate those persons who may have access to the assessments and preclude access to all others. The Act contains criminal penalties for disclosure of a vulnerability assessment to anyone other than an individual designated by the EPA, except in specified, limited circumstances. *Id.* § 300i-2(a)(5).

5. Emergency response plan.

a. Each CWS serving a population greater than 3,300 is required to prepare an emergency response plan that incorporates the results of vulnerability assessments. *Id.* § 300i-2(b).

b. The CWS is not required to submit a copy of its emergency response plan to the EPA, but must instead certify to EPA not later than six (6) months of completing the vulnerability assessment that the system has completed such plan. *Id.*

c. The emergency response plan must include:

- plans, procedures, and identification of equipment that can be implemented or utilized in the event of a terrorist or other intentional attack on the public water system;
- actions, procedures, and identification of equipment which can obviate or significantly lessen the impact of terrorist attacks or other intentional actions on the public health and the safety and supply of drinking water provided to communities and individuals.

Id.

d. The Act requires each CWS to coordinate with existing Local Emergency Planning Committees established under the Emergency Planning and Community Right-to-Know Act (42 U.S.C. §§ 11001 *et seq*.) when preparing or revising its emergency response plan. *Id.*

e. Each CWS must maintain a copy of its emergency response plan for five (5) years after certifying the plan to the EPA. *Id.* § 300i-2(c).

6. Guidance to small public water systems.

a. The Act required the EPA to provide guidance to CWS serving a population of less than 3,300 persons on how to conduct vulnerability assessments, prepare emergency response plans, and address threats from terrorist attacks or other intentional actions that would affect the safety or supply of drinking water or significantly affect the public health. *Id.* § 300i-2(d).

b. The EPA published an eight-page document on its website entitled Water Security Strategy for Systems Serving Populations Less than 100,000/15 MGD or Less, July 9, 2002, *see* http://www.epa.gov/safewater/security/med-small-strategy.pdf. This document summarizes the requirements of CWS under the Bioterrorism Act and sets forth what the EPA intends to do to provide tools, guidance, training, technical assistance, and financial assistance. The EPA otherwise refers persons seeking this information to a variety of other websites sponsored by associations and lists “train the trainer” workshops provided without charge to state, tribal, or local agencies that assist drinking water systems.

7. Financial assistance.

a. The Act authorized the EPA funding to provide financial assistance to CWS to perform vulnerability assessments and prepare emergency

response plans, and to help underwrite the expenses of basic security enhancements. Grants have were made to large systems (i.e., CWS serving a population of 100,000 or more). The EPA will not provide grants to smaller systems but instead used the funds to engage nonprofits associations and organizations to provide training and some technical assistance to smaller CWS.

b. Basic security enhancements include for which such funds may be spent include:

- purchase and installation of equipment for detection of intruders;
- purchase and installation of fencing, gating, lighting, or security cameras;
- tamper-proofing of manhole covers, fire hydrants, and valve boxes;
- rekeying doors and locks;
- improvements to electronic, computer, or other automated systems and remote security systems;
- participation in training programs, and the purchase of training manuals and guidance materials, relating to security against terrorist attacks;
- improvements in the use, storage, or handling of various chemicals;
- security screening of employees or contractor support services.

c. This funding may not be used for personnel costs, or monitoring, operation, or maintenance of facilities, equipment, or systems.

8. Training.

The EPA awarded $1.5 million in grants to five nonprofit training and technical assistance organizations to help improve security at small drinking water systems. Training will be provided at no cost to state, tribal, and local officials in drinking water security, and, in turn, these trained officials will train and provide technical assistance to utilities that serve fewer than 50,000 people. “Train-the-trainer” workshops are being offered free of charge throughout the country to train state, tribal, or local agencies that assist drinking water systems. *See* on-site training schedule at http://www.epa.gov/safewater/security/index.html.

III. Gas Pipelines – Integrity Management.

A. Relevant Statute(s).

Pipeline Safety Improvement Act, Pub. L.107-355, 116 Stat. 2985 (December 17, 2002).

B. Responsible Agency.

Research and Special Programs Administration (RSPA), Department of Transportation, operates the Office of Pipeline Safety.

C. Regulations.

Notice of Proposed Rulemaking to establish a rule requiring operators to develop integrity management programs for gas transmission pipelines that, in the event of failure, could impact high consequence areas (HCA). *See* 68 Fed. Reg. 4278 (January 28, 2003).

D. Agency Guidance.

None.

E. Summary.

1. Overview.

The Pipeline Safety Act requires DOT to issue regulations prescribing standards for pipeline operators' risk analysis and integrity management programs by December 17, 2003. The integrity management program requires a baseline assessment of all pipeline facilities. It requires that assessments be completed no later than 10 years after enactment of the law, and that at least 50 percent of the facilities be assessed no later than five years after the date of enactment. The Act also requires implementation of formal public awareness programs by December 17, 2003.

2. Pipeline integrity management in high consequence areas (gas transmission pipelines).

a. The Pipeline Safety Improvement Act of 2002 amended Title 49 of the United States Code by adding § 60109(c), which directs operators of gas pipeline facilities to implement risk analysis and integrity management programs. Section 60109(c) requires each operator of a gas pipeline

facility to (i) conduct an analysis of the risks to each facility located in a high-density population area (identified pursuant to § 60109(a)(1) and defined in 49 C.F.R. chapter 192), and (ii) implement a written integrity management program for each facility to reduce the potential risks.

b. DOT is required to promulgate regulations not later than December 17, 2003 prescribing standards to direct how operators must conduct a risk analysis implement an integrity management program. Each operator of a gas pipeline facility is required to begin a baseline integrity assessment within 18 months of enactment of the law. *Id.*

c. The Act requires each operator of a gas pipeline facility to conduct an analysis of the risks to each facility of the operator located in a high consequence area (defined in 49 C.F.R. chapter 192).

d. High Consequence Areas (HCA).

- Areas where the potential consequences of a gas pipeline accident may be significant or may do considerable harm to people or property.
- RSPA proposed to expand the current HCA definition to address pipelines located near people living at distances greater than 660 feet from large, high-pressure pipelines. This would provide the same level of protection currently provided, *see* 49 C.F.R. § 192.761(f), for certain population groups, e.g., a facility housing people e who are confined, have impaired mobility or are difficult to evacuate (e.g., hospital, church, school, prison, day care facility, retirement facility) or where 20 or more people congregate at least 50 days in any 12-month period.)
- This area is expanded to 1000 feet if the pipeline is greater than 30 inches in diameter and operates at pressures greater than 1000 psig.

3. Required content of regulations.

a. DOT is required to promulgate regulations addressing the following factors:

i. The minimum requirements for integrity assessment of pipeline facilities.

ii. The type or frequency of inspections or testing of pipeline facilities, in addition to the minimum requirements of the periodic reassessment required at least once every seven years;

iii. The manner in which the inspections or testing are conducted.

iv. The criteria used in analyzing results of the inspections or testing.

v. The types of information sources that must be integrated in assessing the integrity of a pipeline facility as well as the manner of integration.

vi. The nature and timing of actions selected to address the integrity of a pipeline facility.

vii. Such other factors as DOT determines appropriate to ensure that the integrity of a pipeline facility is addressed and that appropriate mitigative measures are adopted to protect HCAs.

49 U.S.C. § 60109(c)(6).

b. The regulations also must ensure that all required inspections are conducted in a manner that minimizes environmental and safety risks, and takes into account the applicable level of protection established by national consensus standards organizations. *Id.*

c. DOT may also prescribe standards requiring an operator of a pipeline facility to include in an integrity management program (1) changes to valves or the establishment or modification of systems that monitor pressure and detect leaks based on the operator's risk analysis; and (2) the use of emergency flow restricting devices.

4. Public Education Programs.

a. Gas pipeline operators assert that the greatest opportunity to improve the safety of natural gas pipelines is in the area of damage caused by a third party, i.e., someone other than the operator. The one-call system was put into place to notify operators of damaged pipelines. Parties who cause or notice damage to a pipeline are encouraged to call a telephone number provided by pipeline operators to report damage or accidents.

b. Each owner or operator of a gas or hazardous liquid pipeline facility must carry out a continuing program to educate the public on the use of a one-call notification system prior to excavation and other damage prevention activities, the possible hazards associated with unintended

releases from the pipeline facility, the physical indications that such a release may have occurred, what steps should be taken for public safety in the event of a pipeline release, and how to report such an event. 49 U.S.C. § 60116(a).

c. The program must include activities to advise affected municipalities, school districts, businesses, and residents of pipeline facility locations. 49 U.S.C. § 60116(b).

6. Status of regulations.

RSPA published a notice of proposed rulemaking on January 28, 2003. The comment period on the proposed pipeline integrity management rule closed on April 30, 2003. Final rule has not been published.

IV. Transport of Hazardous Material by Rail.

A. Relevant Statute(s).

Safe Explosives Act of 2002 ("SEA"), Pub. L. 107-296, 116 Stat. 2280 (November 25, 2002), amending 18 U.S.C. 842(i).

B. Responsible Agencies.

Research and Special Programs Administration of the Department of Transportation (RSPA); Federal Railroad Administration of the Department of Transportation (FRA); Transportation Security Administration (TSA) of the Department of Homeland Security; Office of Maritime and Land Security.

C. Regulations.

1. 68 Fed. Reg. 14510 (March 25, 2003) *Hazardous Materials: Security Requirements for Offerors and Transporters of Hazardous Materials; Final Rule* (HM-232), amending 49 C.F.R. Part 172: RSPA's final rule requires persons who offer certain hazardous materials for transportation in commerce and persons who transport certain hazardous materials in commerce to develop and implement security plans. The rule also includes new security awareness training requirements for all hazardous materials employees. The training must include an awareness of the security risks associated with hazmat transportation, measures designed to enhance transportation security, and a component covering how to recognize and respond to possible security threats.

2. 68 Fed. Reg. 34470 (June 9, 2003) *Hazardous Materials: Transportation of Explosives by Rail*: RSPA, FRA, and TSA published this notice to explain that, in light of the extensive regulations of the rail transportation of hazardous

materials, including explosives, by the Department of Transportation, the protections inherent in railroad operations against improper use of those materials by railroad employees, and the security safeguards taken by the railroads, the transportation of explosives via rail by certain persons described under the Safe Explosives Act does not pose a sufficient security risk warranting further regulations at this time.

D. Agency Guidance.

1. 67 Fed. Reg. 6963 (February 14, 2002) *Advisory Notice; Enhancing the Security of Hazardous Materials in Transportation*: RSPA published an advisory notice to inform shippers and carriers of voluntary measures that can enhance the security of hazardous materials shipments during transportation

2. Risk Management Self-Evaluation Framework (RMSEF) by RSPA. *See Enhancing Security of Hazardous Materials Shipments Against Acts of Terrorism or Sabotage Using RSPA's Risk Management Self-Evaluation Framework*, January 2002, available at http://hazmat.dot.gov/rmsef.htm.

E. Summary.

1. Transportation of HAZMAT by rail.

a. RSPA, FRA, and TSA recently announced that employees involved in the transport of explosives by rail would not be required to obtain background checks such as those imposed for employees in the aviation industry and motor vehicle operators holding hazmat endorsements to commercial drivers licenses. *See* 68 Fed. Reg. 34470 (June 9, 2003).

b. The notice provides that additional regulation of rail transportation of hazardous materials is not warranted at this time. TSA determined that additional regulations concerning railroad employees are not warranted at this time because of the conditions under which explosives are transported by rail and the difficulty that a potential criminal or terrorist would have in gaining access to or controlling an explosives shipment. *See Id.* at 34476. TSA "continues to assess the need for more detailed background check requirements in the rail industry and may determine that such standards are necessary in the future." *Id.*

c. TSA took this position in part because of the protections inherent in railroad operations against improper use of those materials by railroad employees and the security safeguards taken by the railroads. More than 75 percent of hazmat shipped by rail moves in bulk. The hazmat is loaded into the tank, hopper or boxcar by the shipper and then delivered to the railroad for movement to its destination. Railroad employees do not load or unload hazmat. To arrange for the rail transport of hazmat, the shipper

must provide a shipping description of the hazmat, including emergency response information to the railroad. The shipper must also certify that the materials to be shipped have been classified, packaged, and labeled appropriately and are in proper condition for transportation according to DOT standards, including proper placarding. Shippers often apply security seals to shipping containers. *Id.* at 34474.

d. The notice concludes that "because of the conditions under which explosives are transported by rail and the difficulty that a potential criminal or terrorist would have in gaining access to or controlling an explosives shipment and the other Federal and industry measures currently in effect, we do not believe that additional regulations concerning railroad employees are warranted at this time." *Id.* A significant factor in this decision is the fact that unlike a truck or aircraft, a train operates on a closed system. It is confined to the tracks, moved along a pre-designated route, and remains in communication with the railroad so that an alteration of the route would be detected quickly. *Id.* at 34475.

2. GAO report.

a. The GAO recently issued a report on rail security. *See* Rail Safety and Security- Some Actions Already Taken to Enhance Rail Security, but Risk-based Plan Needed, GAO-03-435 (May 23, 2003).

b. TSA has begun work on an overall intermodal transportation system security plan, but has not yet developed a plan to specifically address the security of individual surface transportation modes, including rail, and does not have time frames established for completing such an effort." *Id.* at 10. TSA intends to develop a risk-based management approach to identify "threats that exist to the shipment of hazardous materials by rail, vulnerabilities that may be exploited in the system used to ship these materials, and high-risk, high-consequence facilities that need protection." *Id.*

c. The GAO report noted that chemical manufacturers are required to notify their communities of the existence of hazardous materials at their facilities. DOT, however, has not yet addressed whether to require companies to notify community emergency response officials when hazardous materials being shipped by rail are stored in transit in the community.

3. Increasing security of HAZMAT in transportation.

RSPA published an advisory notice to inform shippers and carriers of hazardous materials of voluntary measures that can enhance the security of hazardous materials shipments during transportation. See 67 Fed.

Reg. 6963 (Feb. 14, 2002). RSPA recommended that shippers and carriers implement the following measures:

i. Security plan that uses a risk management model to assess security risks and develop appropriate measures to reduce or eliminate the risk. *Id.* at 6964.

ii. Personnel Security: involves assuring employees of the industry are familiar with security plan and properly trained in its implementation, encouraging employees to report suspicious incidents and events, implementing routine security inspections, and establishing an internal communication system to inform staff of events, facts, trends and updates. *Id.* at 6964.

iii. Facility Security: RSPA encourages the railroad industry to consider establishing various security measures to prevent unauthorized access to the facility. *Id.* at 6964. Some of the measures are: establishing partnerships with local law enforcement officials, restricting the availability of information related to facility and the materials it handles, adding security guards and increasing off-hours patrol, improving fencing around the facility, installing additional lights, alarm systems and surveillance cameras, placing limits on visitor access, conducting security spot checks of personnel and vehicles. *Id.* at 6964-65.

iv. En Route Security: Shippers and carriers should consider various security measures to assure the security of hazardous materials shipments en route from origin to destination. *Id.* at 6965. Some measures include: establishing advance technology to track or protect shipments, establishing a communication system with transport vehicles and operators, implementing a system for a customer to alert the shipper if a hazardous materials shipment is not received when expected, training drivers in how to avoid high jacking, identifying preferred and alternative routing. *Id.*

4. Preparation of security plan and employee security training.

a. RSPA's rule requires persons who offer certain hazardous materials for transport in commerce, in amounts that require placarding, and persons who transport certain hazardous materials in commerce to develop and implement written security plans, and to train hazmat employees in security awareness. 68 Fed. Reg. 14510 (March 25, 2003). RSPA seeks to "characterize a security plan in terms of addressing and reducing security risks presented by the transportation of certain hazardous materials in commerce." *Id.* at 14513-14.

b. The requirement for a security plan sets forth general requirements for a security plan's components rather than a prescriptive lists of specifics that must be included in order to insure that the security plan can be adopted to a specific industry's needs. *Id.* at 14515. Those subject to this rule must perform risk assessments of transportation security. *Id.* at 14516. The security plan must include an assessment of possible transportation security risks for the materials to be transported and appropriate measures to address identified risks. *Id.* It must also "include a method or methods for confirming information provided by applicants for jobs that involve access to or handling of the hazardous materials covered by the plan." *Id.* In addition, the plan "must also include methods to address the possibility that unauthorized persons may attempt to gain access to hazardous materials or transport vehicles being prepared for transportation." *Id.* Furthermore, the security plan must include "a method or methods to address en route security risks." *Id.*

V. Is Sensitive Information Protected by Federal Law Safe From Disclosure Under State Right to Know Laws?

A. Community Water Systems (Title IV of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, amending the Safe Drinking Water Act)

1. Vulnerabilities Assessments of community water systems under the amended Safe Drinking Water Act are to be submitted to the Administrator. The amendments further provide, "Except for information contained in a certification under this subsection identifying the system submitting the certification and the date of the certification, all information provided to the Administrator under this subsection and all information derived therefrom shall be exempt from disclosure under section 552 of title 5 of the United States Code [Freedom of Information Act]." Public Law 107-188, sec. 401, 116 Stat. 682 (June 12, 2002).

2. The amendments further provide, "No community water system shall be required under State or local law to provide an assessment described in this section to any State, regional, or local government entity solely by reason of the requirement … that the system submit such assessment to the Administrator." *Id.*

B. Risk Management Program under Section 112(r) of the Clean Air Act.

1. Section 112(r) of the Clean Air Act requires facilities handling toxic, flammable and explosive substances to develop a risk management program containing information on facility identity, off-site consequence analysis, the facility's accident history for the past five years, a prevention program, and an emergency response program. 42 U.S.C. § 7412(r). In the context of examining

off-site consequences, the facility must assess the off-site consequences of a "worst-case scenario" describing the potential consequences to the public and environment of a catastrophic release.

2. In 1999 Congress enacted the Chemical Safety Information, Site Security and Fuels Regulatory Relief Act (Public Law 106-40) amending section 112(r) of the Clean Air Act to limit public access to the worst-case scenario information. This off-site consequence analysis is available to an officer or employee of a State or local government. 42 U.S.C. 7412(r)(7)(H)(i), (ii). The Clean Air Act also provides that this subparagraph (and the regulations thereunder) supercede any provision of State or local law that is inconsistent with the subparagraph (or its regulations). *Id.* at 7412(r)(7)(H)(x)(I). However, "[n]othing in this subparagraph precludes a State from making available data on the off-site consequences of chemical releases collect in accordance with State law." *Id.* at 7412(r)(7)(H)(x)(II).

C. Emergency Planning and Community Right to Know Act.

Any information received by a state or local government under the Emergency Planning and Community Right-To-Know Act, 42 U.S.C. § 11001 *et seq.*, ordinarily will be available under a state's right to know law. The Act expressly provides that "Nothing in this chapter shall…preempt any State or local law." 42 U.S.C. § 11041.

VI. Transportation of Hazardous Material by Motor Vehicle.

A. *See* U.S. Departments of Homeland Security and Transportation Issue New Rules Requiring Background Records Checks Prior to Licensing Operators of Vehicles that Transport Hazardous Materials, HOMELAND SECURITY BULLETIN, by Craig P. Wilson, Barry M. Hartman, Marsha A. Sajer, June 2003.

B. Update:

States and trade associations have written to TSA and FMCSA seeking a delay in implementing regulations requiring transporters of hazardous materials to receive background checks. Many states have indicated they are unable to meet deadlines requiring them to implement the fingerprint-based background checks before the November 3, 2003, deadline. The state DMVs lack time, finances, and specific TSA and FMCSA regulatory guidance to put hardware, software, and procedures in place. Some states also have procurement laws that require state agencies to award contracts for the implementation of these systems only after a competitive bidding process.

The states have justified their request for delay of the implementation deadline noting that the assessment process will require the coordination and cooperation of a number of different agencies at the federal, state, and local level, yet FMCSA and TSA provided only general guidelines in such key areas as the collection and processing of fingerprints, submission of applications and collection of fees, notification of assessments to applicants and states, record retention requirements for states, and the handling of appeals, extensions, and waivers. The rule requires states to give drivers 180 days notice that they must initiate procedures before the expiration of their hazardous materials endorsement but few if any states have begun sending these notices.

VII. Security of Chemical Manufacturing Facilities.

See Senate Considers Competing Bills to Address Security at Chemical Manufacturing and Processing Facilities, HOMELAND SECURITY BULLETIN, by Barry M. Hartman, Craig P. Wilson and Tom Manganello, July 2003.

VIII. Security of Marine Facilities.

See Homeland Security Spurs New Regulatory Requirements for Over 5000 Businesses with Facilities Near Ports, Rivers, Lakes, Streams and Wetlands, HOMELAND SECURITY BULLETIN, by Barry M. Hartman, Craig P. Wilson and John A. Orlowski, September 2003.

BARRY M. HARTMAN
bhartman@kl.com
202.778.9338

CRAIG P. WILSON
cwilson@kl.com
717.231.4509

MARSHA A. SAJER
msajer@kl.com
717.231.5849

Kirkpatrick & Lockhart LLP Homeland Security Bulletins:

Homeland Security Expands to regulation of the Manufacture, Use, Transportation, and Disposal of Hazardous Substances and Materials, Including Chemical and Biological Agents, HOMELAND SECURITY BULLETIN, by Barry M. Hartman, Christopher E. Dominguez, Marsha A. Sajer, April 2003.



hsb_2003.pdf

U.S. Departments of Homeland Security and Transportation Issue New Rules Requiring Background Records Checks Prior to Licensing Operators of Vehicles that Transport Hazardous Materials, HOMELAND SECURITY BULLETIN, by Craig P. Wilson, Barry M. Hartman, Marsha A. Sajer, June 2003.



usdept_0603.pdf

Senate Considers Competing Bills to Address Security at Chemical Manufacturing and Processing Facilities, HOMELAND SECURITY BULLETIN, by Barry M. Hartman, Craig P. Wilson and Tom Manganello, July 2003.



senateconsiders_0703.pdf

Homeland Security Spurs New Regulatory Requirements for Over 5000 Businesses with Facilities Near Ports, Rivers, Lakes, Streams and Wetlands, HOMELAND SECURITY BULLETIN, by Barry M. Hartman, Craig P. Wilson and John A. Orlowski, September 2003.



hsb_0903.pdf