



Newsletter

April, 2005
No. 2

Energy and Maritime Law

In This Issue

R. Bruce Barze, Jr. is a partner in the Litigation Section of BALCH & BINGHAM LLP and is Chair of the IADC Energy and Maritime Law Committee.

Jeffrey H. Wood is an associate in the Environmental & Natural Resources Section of BALCH & BINGHAM LLP.

Securing the Homeland: Recent Developments in Maritime & Energy Policy

By R. Bruce Barze, Jr. and Jeffrey H. Wood

In the wake of the September 11 tragedies, President Bush issued the NATIONAL STRATEGY FOR HOMELAND SECURITY in 2002 to “mobilize and organize our Nation to secure the U.S. homeland from terrorist attacks.” Several months later, the President signed into law the Homeland Security Act of 2002 (“HSA”), which initiated the largest reorganization of federal agencies in over fifty years by transferring offices from within the Departments of Treasury, Justice, Transportation, Agriculture, Energy, and Defense to the newly-created Department of Homeland Security (“DHS”). This article is designed to update lawyers practicing in the maritime and energy arenas regarding the evolving relationships between the more traditional departments and the DHS.

The IADC

The IADC dedicates itself to enhancing the development of skills, professionalism and camaraderie in the practice of law in order to serve and benefit the civil justice system, the legal profession, society and our members.

Department of Homeland Security

The Department of Homeland Security was commissioned to, among other things, prevent and respond to terrorist attacks within the United States, and act as a focal point for natural disasters and emergencies. *See* 6 U.S.C. § 111. The HSA divided the DHS into five directorates each headed by an under-secretary: (1) Border and Transportation Security; (2) Emergency Preparedness and Response; (3) Science and Technology; (4) Information Analysis and Infrastructure Protection; and (5) Management. In addition, the United States Coast Guard is located within the DHS and reports directly to the Secretary. DHS recently published a new strategic plan outlining its approach to securing the homeland. *See* SECURING OUR HOMELAND: U.S. DEPARTMENT OF HOMELAND SECURITY STRATEGIC PLAN (2004).

International Association of Defense Counsel
One North Franklin, Chicago, IL 60606

Phone: (312) 368-1494 Fax: (312) 368-1854 Email: cbalice@iadclaw.org www.iadclaw.org

Border & Transportation Security Directorate

The Border & Transportation Security Directorate – DHS’s largest directorate – brings the nation’s major border security and transportation agencies under one roof. The agencies (or parts of these agencies) transferred to this directorate include the U.S. Customs Service, the Immigration & Naturalization Service, the Transportation Security Administration (“TSA”), and the Animal & Plant Health Inspection Service. This directorate is responsible for preventing the entry of terrorists and terrorist weapons by securing the borders, ports, waterways, and airports. *See* 6 U.S.C. § 202. This directorate also oversees the agricultural import and entry inspection activities under the Endangered Species Act. *See id.* § 231. Importantly, while the TSA is responsible for hazmat enforcement at the nation’s borders and airports, the Department of Transportation remains actively involved in securing hazardous materials transported in commerce. *See* Hazardous Materials: Security Requirements for Offerors and Transporters of Hazardous Materials, 68 Fed. Reg. 14,510 (2003) (final rule).

Emergency Preparedness & Response Directorate

The Emergency Preparedness & Response Directorate oversees domestic disaster preparedness training and coordinates government disaster response. *See* 6 U.S.C. § 311. Included within this directorate are the Federal Emergency Management Agency (“FEMA”), the Nuclear Incident Response Team, and various other disaster preparedness agencies. *See id.* § 313. Specifically, this directorate helps “to ensure the effectiveness of emergency response providers to terrorist attacks, major disasters, and other emergencies,” and disburses funds to the Department of Energy for homeland security activities. *Id.* § 312. *Homeland Security Presidential Directive 8*, which was issued on December 17, 2003,

establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies, and describes the way federal departments and agencies will prepare for such events. In addition, *Homeland Security Presidential Directive 9*, which was issued on February 3, 2004, establishes a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies.

Science & Technology Directorate

The Science & Technology Directorate now houses the CBRN Countermeasures Programs and the Environmental Measurements Laboratory, among other offices. This directorate is responsible for using all scientific and technological advantages in securing the homeland, which includes operating chemical and biological national security programs, and nuclear smuggling programs. 6 U.S.C. § 183.

Information Analysis & Infrastructure Protection

The Information Analysis & Infrastructure Protection Directorate analyzes intelligence information pertaining to homeland security gathered by various agencies. This directorate brings together the Critical Infrastructure Assurance Office and the Energy Security and Assurance Program. One of the most well-known functions of this directorate is to administer the color-coded Homeland Security Advisory System. *Id.* § 121(d)(7). Also, this directorate is responsible for “develop[ing] a comprehensive national plan for securing key resources and critical infrastructure . . . , including power production, generation, and distribution systems . . .” *Id.* § 121(d)(5).

Subtitle B of Title II of the HSA, known as the Critical Infrastructure Information Act (“CIIA”) (codified at 6 U.S.C. §§ 131 *et seq.*), addresses the circumstances under which DHS may obtain, use, and disclose critical

infrastructure information. Pursuant to CIIA, DHS' Information Analysis & Infrastructure Protection Directorate is preparing to publish a final rule describing its approach to working with the private sector to protect critical infrastructure information. *See* Procedures for Handling Critical Infrastructure Information, 69 Fed. Reg. 8,074 (Feb. 20, 2004) (interim rule). In *Homeland Security Presidential Directive 7*, which was issued on December 17, 2003, President Bush assigned specific infrastructure protection responsibilities to various federal agencies. For example, the Department of Energy must conduct vulnerability assessments for the energy sector, including the production, refining, storage, and distribution of oil, gas, and electric power.

Federal Agency Implementation of the Homeland Security Act

Various federal agencies, including the Energy Department, the Federal Energy Regulatory Commission ("FERC"), the United States Army Corps of Engineers, and the United States Coast Guard, which have significant roles in maritime and energy policy, are bustling to respond to the needs of post-September 11 domestic security.

Department of Energy

Looking to the President's NATIONAL STRATEGY TO SECURE CYBERSPACE, which was issued in 2003, the Energy Department is spearheading efforts to develop best practice techniques and new technologies in both the public and private sectors to thwart security breaches of critical information systems. The Energy Department is also taking steps to protect energy infrastructure pursuant to the President's NATIONAL STRATEGY FOR THE PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURE AND KEY ASSETS issued in 2003. In light of the threat posed by "electromagnetic pulse weapons" and other modern terrorist weaponry, the U.S. Department of Energy's Office of Energy Assurance ("OEA") must work closely

with the DHS and other agencies to ensure the reliable and secure operation of the nation's energy systems. One issue where OEA and DHS are collaborating involves "supervisory control and data acquisition" ("SCADA") networks, which are the computer systems that perform key functions in delivering electricity to the country. As a critical component of the nation's energy infrastructure, these systems are especially attractive targets to terrorists, and as a result, OEA is currently exploring approaches to secure these and other systems used to monitor and control equipment in energy facilities.

FERC

In its STRATEGIC PLAN FOR FISCAL YEARS 2003-2008, the Federal Energy Regulatory Commission describes its current and future plans for addressing the security of natural gas pipelines and hydropower projects. For example, FERC adopted a rule on the identification and handling of critical energy infrastructure information. *See* 68 Fed. Reg. 9,857 (Mar. 3, 2003). FERC has also identified hundreds of dams that necessitate greater security. In coordination with the U. S. Coast Guard, FERC is addressing issues regarding security at waterfront liquefied natural gas (LNG) facilities.

U.S. Army Corps of Engineers

Given that the Corps manages 75 hydroelectric power plants, over 500 dams, and almost 1,000 harbors, the importance of the Corps to protecting the nation's critical infrastructure cannot be understated, especially considering the potential impact of large power outages, dam failures, water supply contamination, or the import of weapons of mass destruction via harbors and waterways. Recently, the Corps developed policies to ensure that national security concerns are adequately considered when reviewing harbor and inland harbor projects. *See* Corps Memorandum re: National Security Consideration in the Planning, Design, Construction, and Operation and Maintenance of Harbor and Inland Harbor Projects (June 30,

2003). *See also* 69 Fed. Reg. 42,258 (July 29, 2004) (establishing a new restricted area in the waters near Mobile Bay). Also, in December 2002, the Corps established the Homeland Security Office within the Corps' Civil Works Directorate, which the Corps uses to support the homeland security needs of the Army, Department of Defense, and DHS. Moreover, the Corps continues to manage – as it did before September 11 – various programs aimed at protecting critical infrastructure. Much of the Corps' homeland security efforts are chronicled in its CIVIL WORKS STRATEGIC PLAN (March 2004).

U.S. Coast Guard

Having worked closely with the DOJ and FBI in traditional criminal enforcement for many years, the United States Coast Guard – now housed under the DHS – remains actively involved in many aspects of homeland security. The Coast Guard's role became even more important with the enactment of the Maritime Transportation Security Act of 2002 ("MTSA"), Pub. L. No. 107-295, 116 Stat. 2064 (2002), which required extensive evaluations of the nation's transportation security. Specifically, the MTSA called for the development of "vulnerability assessments," which would evaluate the various security threats posed to maritime vessels, and "security plans," which would outline strategies for deterring and responding to breaches of transportation security. *See* 46 U.S.C. § 70103.

Following the MTSA, the Coast Guard developed its MARITIME STRATEGY FOR HOMELAND SECURITY in December of 2002 to provide a framework to accomplish the Coast Guard's strategic objectives. The Maritime Strategy is focused on protecting U.S. population centers, critical infrastructure, maritime borders, ports, and coastal areas. The Coast Guard has recently taken several steps in accordance with its Maritime Strategy. For instance, the Coast Guard amended its regulations to increase its ability to protect the nation's ports by requiring

vessels carrying hazardous materials to implement security plans. *See* 33 C.F.R. pt. 104 (as amended by 68 Fed. Reg. 60,448 (2003)). Also, the Coast Guard continues to extensively regulate vessels carrying oil, noxious liquid substances, and other hazardous substances and materials. *See* 33 C.F.R. pts. 151-159. Finally, pursuant to the Magnuson Act, 50 U.S.C. §§ 191 *et seq.*, the Coast Guard may establish security zones around critical infrastructures near the nation's coasts, such as power plants, to protect against terrorist attacks. *See, e.g.*, 68 Fed. Reg. 75,134 (2003) (temporary final rule) (establishing a security zone around a liquefied natural gas terminal located on Chesapeake Bay).