THE GOVERNMENT CONTRACTOR®

THOMSON WEST

Information and Analysis on Legal Aspects of Procurement

Vol. 45, No. 10 March 12, 2003

Developments

¶ 107

EO Implements Transition To DHS; Changes Infrastructure Protection System And Contractor Indemnification Rules

A February 28 Executive Order to reassign authorities related to the Department of Homeland Security transition inserts a few significant changes to security-related issues along the way. The order, EO 13286, was published in the *Federal Register* on March 5 (68 Fed. Reg. 10619) and primarily lists amendments to previous EOs to substitute appropriate DHS officials for security authorities and advisory bodies formerly held by the new department's component agencies. In the course of these administrative changes, however, the EO eliminates the President's Critical Infrastructure Protection Board (PCIPB) and may affect the Department of Defense's authority to indemnify homeland security contractors under P.L. 85-804 (See Practitioner Comment, below).

In § 7, the order amends EO 13231 of October 16, 2001 to remove all traces of the PCIPB. The Board was originally created with members from Cabinet-level and executive agencies to coordinate the protection of information systems for infrastructure deemed critical by agencies, state and local governments, corporations, and academic institutions. See 43 GC ¶ 406. Among other things, the Board was responsible for acting as liasion between the Office of Science and Technology Policy, the National Science Foundation, and the Defense Advanced Research Projects Agency on the research and development of new security information systems.

The elimination of the PCIPB has raised concerns that the recommendations and directives in the recent National Strategy to Secure Cyberspace (see 44 GC ¶ 367 and 45 GC ¶ 83) will not have enough support from a centralized Government body to make the changes happen. The Information Technology Association of America President, Harris N. Miller, said the "PCIPB, which consists of the top leadership from throughout the federal government, reflects a fundamental fact: cyber security requires the participation of all government entities, and the coordination facilitated by the CIPB is essential." The Homeland Security Department will now take the lead on advising the President and coordinating with both the private and public sectors regarding infrastructure security. The DHS will accomplish these tasks through the National Infrastructure Advisory Council (NIAC), which was also created by the October 16, 2001 EO. The NIAC will have up to 30 members, appointed by the President, from across the Government, private industry, and academia.

In addition to terminating the PCIPB, the EO grants the DHS Secretary the same responsibilities previously held by individual agency officials, such as ordering selected military reservists to active duty (Secretary of Transportation) and assigning emergency preparedness responsibilities (Secretary of the Federal Emergency Management Agency). Further, § 73 of the EO authorizes the DHS Secretary to provide indemnification under P.L. 85-804, under limited circumstances, to contractors performing unusually hazardous activities. The potential impact of the change is discussed in the below Practitioner Comment.

✦ **Practitioner Comment**—Section 73 of the Executive Order significantly changes the landscape for contractors involved in homeland security activities who wish to take advantage of P.L. 85-804. Under the new EO, the Secretary of Homeland Security is authorized to provide in-

demnification under P.L. 85-804. But what the EO gives with one hand, it takes away with the other. Specifically, while the order gives the new agency authority to provide P.L. 85-804 indemnifications, it prohibits using P.L. 85-804 for "any matter that has been, *or could be*, designated …as a qualified anti-terrorism technology" under the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act), which is incorporated in the Homeland Security Act. The universe of what "could be" designated an anti-terrorism technology is certainly open-ended, and "could be" quite broad. Thus, a large universe of unusually hazardous activities may be relegated to the umbrella of the SAFETY Act. The SAFETY Act offers a mechanism for contractors who sell "qualified anti-terrorism technologies" to limit their liability in the event of a terrorist act. However, the SAFETY Act is not nearly as comprehensive as P.L. 85-804 because it offers no indemnification and is only triggered by a terrorist act—not by an unusually hazardous risk.

The order does provide some exceptions. First, DOD may continue to utilize P.L. 85-804 authority, but only if, after taking into consideration the SAFETY Act, the Secretary of Defense concludes that the indemnification "is necessary for the timely and effective conduct of United States military or intelligence activities." Second, all other agencies with P.L. 85-804 authority will be required to consult the Secretary of Homeland Security and obtain OMB approval before providing an indemnification. While the language is not clear, the Secretary of Homeland Security will presumably advise the requesting agency whether the SAFETY Act (rather than P.L. 85-804) is a more appropriate authority. The strong implication here is that any technologies that "could" qualify under the SAFETY Act will not be eligible for indemnification under P.L. 85-804.

Issuance of this order signals the Administration's strong preference for the use of the SAFETY Act over P.L. 85-804 for homeland security projects. This approach fails to consider the range of liabilities associated with unusually hazardous activities that have been covered under P.L. 85-804 for nearly 50 years. Indeed, many of the risks associated with homeland security projects relate to the possibility of technological failures or human errors in implementing innovative, and often hazardous, technologies. Therefore, contractors engaged in unusually hazardous activities, who wish to preserve their ability to obtain protection under P.L. 85-804, need to consider whether the SAFETY Act's designation of "qualified anti-terrorism technology" will limit or enhance their risk mitigation options.

✥

This PRACTITIONER COMMENT was written for THE GOVERNMENT CONTRACTOR by Agnes P. Dover, a partner in the Washington, D.C. office of Hogan & Hartson, LLP. Ms. Dover is also a member of THE GOVERNMENT CONTRACTOR Advisory Board.