

# Homeland Security Bulletin

MARCH 2003

This Homeland Security Bulletin is the initial publication of the Homeland Security practice group at Kirkpatrick & Lockhart LLP. Future issues will address ongoing legislative, judicial and regulatory developments, including in the areas of procurement, government contracting, criminal investigations and information security. We welcome your comments on this Bulletin, as well as your questions on the topics covered.

## The Homeland Security Act of 2002—A Summary

### OVERVIEW

On November 25, 2002, President Bush signed into law the Homeland Security Act of 2002 (“Act”).<sup>1</sup> In consideration of the breadth of the Act’s intended goals “to defend the United States and protect citizens from the dangers of a new era,” as declared by President Bush, the Act will have a significant impact on America. This summary sets forth the structure of the Act and describes the key reorganizations that will occur.

The Act creates a new federal agency, the Department of Homeland Security (“DHS”), which will combine 22 existing and separate federal agencies, including the Immigration and Naturalization Service, the Secret Service, the Customs Service, the Federal Emergency Management Administration and the Border Patrol. DHS will be headed by a Secretary of Homeland Security (“Secretary”) appointed by the President.<sup>2</sup> The initial Secretary is former Pennsylvania governor Thomas Ridge. The primary mission of DHS shall include pursuit of the following objectives:

- preventing terrorist attacks within the United States;
- reducing the vulnerability of the United States to terrorism;
- minimizing the damage, and assist in the recovery, from domestic terrorist attacks;
- carrying out all functions of various entities transferred to DHS; and
- ensuring that the overall economic security of the United States is not diminished by homeland security efforts, activities and programs.<sup>3</sup>

### ORGANIZATION OF THE ACT

The Act establishes the following seven major functions for DHS:

- information analysis and infrastructure protection;
- procurement, and the advancement of science and technology, in support of homeland security;
- border and transportation security;
- emergency preparedness and response;
- coordination with other branches of the federal government, state and local governments and the private sector;
- establishment of the National Homeland Security Council; and
- information security.

Additionally, DHS will continue to implement other functions of the agencies it will absorb.<sup>4</sup> For each major function, a separate Title of the Act addresses administrative procedures related to the performance of each function, as well as substantive legal structures required to enhance the ability of DHS to perform those functions. The following is a summary of the Act’s provisions regarding each major function.

### TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

#### Subtitle A—Directorate for Information Analysis and Infrastructure Protection; Access to Information

In furtherance of the Act’s mission, an Under Secretary for Information Analysis and Infrastructure Protection shall be appointed to develop a comprehensive national

plan both to assess the nature and scope of any vulnerability of key resources and “critical infrastructures” through receiving, analyzing and integrating relevant law enforcement information, intelligence and other information, as well as to identify, implement and support protective measures.<sup>5</sup>

For purposes of the Act, “critical infrastructure” means either physical or virtual systems and assets that are “vital to the United States” and whose incapacity or destruction “would have a debilitating impact on security, national economic security, national public health or safety.”<sup>6</sup> Specifically, the Under Secretary is responsible for establishing “a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools” in order to handle and disseminate data relating to critical infrastructures (see Subtitle B, The Critical Infrastructure Information Act).<sup>7</sup> The Directorate for Information Analysis and Infrastructure Protection must coordinate training and other support to various federal, state and local government personnel to facilitate the appropriate identification and sharing of such information.<sup>8</sup>

The Secretary of DHS is broadly authorized to consult with the private sector to “ensure appropriate exchanges of information” relating to threats of terrorism in the United States, including those related to law enforcement.<sup>9</sup> The Secretary is entitled to receive the following three broad categories of intelligence and other information “collected, possessed, or prepared” by any agency or department of the federal government:

- Any reports, assessments and analytical information relating to threats of terrorism in the United States or to other areas governed by DHS (including any work product of law enforcement, intelligence and other government agencies);
- Any information concerning infrastructure or other vulnerabilities of the United States to terrorism (including certain unprocessed or “raw” data or information); and
- Any unprocessed or “raw” data or information on subjects other than those relating to infrastructure or other vulnerabilities of the United States to terrorism.<sup>10</sup>

For the first and second categories of information listed above, federal agencies are required to furnish such material to the Secretary without request, except where

the President directs otherwise. With respect to the third category of information, the Secretary has the right to receive such information only as the President instructs.<sup>11</sup> In all cases, the Secretary shall be provided by law enforcement agencies such terrorism-related information that is currently required to be provided to the Director of Central Intelligence.<sup>12</sup>

## Subtitle B—The Critical Infrastructure Information Act

Within the Act, the Critical Infrastructure Information Act of 2002 encourages the sharing of information with DHS by the private sector, state and local governments and individuals. It provides for the designation by either the President or the Secretary of a critical infrastructure protection program from an existing component or bureau of a federal agency to receive critical infrastructure information.<sup>13</sup> Under Section 212(3) of the Act, the term “critical infrastructure information” is defined as “information not customarily in the public domain and related to the security of critical infrastructure or protected systems,”<sup>14</sup> including (a) any actual or potential physical or computer-based attack, (b) the ability of any critical infrastructure or protected system to resist such compromise, or (c) any planned or past operational problem or solution related to such compromise, including repair or insurance.

Critical infrastructure information that is voluntarily submitted to DHS for use in the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution or other informational purpose (including the identity of the submitting person or entity) is not subject to public disclosure under the Freedom of Information Act<sup>15</sup> and other federal and state disclosure requirements, when accompanied by an express statement that such information is being submitted voluntarily in expectation of such nondisclosure protection.<sup>16</sup> To this end, the Secretary is required to establish certain procedures for the receipt, care and storage by federal agencies of voluntarily submitted critical infrastructure information; the unauthorized disclosure of such information shall be subject to criminal penalty.<sup>17</sup>

Additionally, the federal government is authorized to issue advisories, alerts and warnings to certain relevant companies, targeted sectors, other governmental entities or the general public regarding potential threats to critical infrastructure, but shall take appropriate steps to

protect from disclosure the source of such information and any related proprietary or sensitive information.<sup>18</sup>

### Subtitle C—Information Security

The Secretary is required to establish procedures on the use of information shared under Title II of the Act that:

- limit its re-dissemination for an unauthorized purpose;
- ensure its security and confidentiality;
- protect the constitutional and statutory rights of the individual subjects of such information; and
- provide data integrity by timely removing and destroying obsolete or erroneous names and information.<sup>19</sup>

Also, the Secretary must appoint a senior DHS official to assume primary responsibility for information privacy policy.<sup>20</sup>

In carrying out the objectives of the Directorate for Information Analysis and Infrastructure Protection, the Under Secretary is required to provide: (1) to state and local governments and, upon request, to private entities that own or operate critical information systems, analysis and warnings related to threats to and vulnerabilities of such systems, as well as crisis management support in response to threats to or attacks of such systems; and (2) technical assistance, upon request, to private sector and other government entities with respect to emergency recovery plans to respond to major failures of such systems.<sup>21</sup> Additionally, the Under Secretary is authorized to establish a national technology guard (referred to as “NET Guard”) to assist local communities to respond to and recover from attacks on information systems and communications networks.<sup>22</sup>

Within the Act, the Cyber Security Enhancement Act of 2002 requires enhanced criminal penalties in cases involving fraud in connection with computers and access to protected information, protected computers, or restricted data in interstate or foreign commerce or involving a computer used by or for the federal government, except where such electronic communication stems from the good faith belief that an emergency involving the threat of death or serious physical injury may result without such immediate disclosure to government authorities.<sup>23</sup>

### Subtitle D—Department of Justice Office of Science and Technology

The Act establishes within the Department of Justice (“DoJ”) an Office of Science and Technology (“OST”). The OST is not within DHS, but has a closely aligned mission to: (1) serve as the national focal point for work on law enforcement technology (e.g., investigative and forensic technologies); and (2) implement programs that improve the safety and effectiveness of such technology and improve technology access by federal, state, and local law enforcement agencies.<sup>24</sup> Specific duties of the OST include:

- establishing and maintaining technology advisory groups and performance standards;
- conducting research, development, testing, evaluation, and cost-benefit analyses for improving the safety, effectiveness, and efficiency of technologies used by federal, state, and local law enforcement agencies; and
- operating existing regional National Law Enforcement and Corrections Technology Centers and establishing additional centers through a merit-based, competitive process.<sup>25</sup>

Additionally, the Attorney General is authorized to transfer to the OST any other DoJ program or activity determined to be consistent with its mission.<sup>26</sup>

### Functions Transferred

Certain federal agencies and functions related to information analysis and infrastructure protection that are transferred to DHS include:

- the National Infrastructure Protection Center (“NIPC”) of the Federal Bureau of Investigation (other than the Computer Investigations and Operations Section);
- the National Communications System of the Department of Defense;
- the Critical Infrastructure Assurance Offices of the Department of Commerce;
- the National Infrastructure Simulation and Analysis Center of the Department of Energy and its energy security and assurance program; and
- the Federal Computer Incident Response Center of the General Services Administration.

## Title III—Science and Technology Advances

In furtherance of the Act's mission, an Under Secretary for Science and Technology (Dr. Charles E. McQueary has been identified as the initial Under Secretary) shall be appointed to direct, fund, conduct and coordinate national research, development and procurement efforts in support of homeland security, including measures seeking to (a) prevent the importation of terrorist weapons and material and (b) detect, prevent, protect against, and respond to terrorist attacks, by:

- developing in coordination with other appropriate executive agencies as well as the federal government's "civilian efforts" a national plan for identifying countermeasures to chemical, biological, radiological, nuclear and other emerging terrorist threats;
- assessing and testing homeland security vulnerabilities and possible threats in support of the Under Secretary for Information Analysis and Infrastructure Protection;
- conducting basic and applied research, development, demonstration, testing and evaluation activities relevant to homeland security objectives, excluding certain human health-related research and development activities;
- establishing a system for disseminating homeland security developments and technologies to federal, state, local government and private sector entities; and
- entering into agreements or otherwise collaborating with the Department of Energy ("DoE"), the Department of Agriculture, the Department of Health and Human Services ("HHS") and the Attorney General in furtherance of the above.<sup>27</sup>

With respect to civilian human health-related R&D activities relating to HHS countermeasures for chemical, biological, radiological, and nuclear and other emerging terrorist threats, the HHS Secretary is required to: (1) set priorities, goals, objectives, and policies and develop a coordinated strategy for such activities in collaboration with the DHS Secretary to ensure consistency with the national policy and strategic plan; (2) collaborate with the DHS Secretary in developing specific benchmarks and outcome measurements for evaluating progress toward achieving such priorities and

goals; and (3) specify the substances to be considered countermeasures.<sup>28</sup> Additionally, the HHS Secretary is authorized to declare when an actual or potential bioterrorist incident or other public health emergency makes advisable the administration of a covered countermeasure against smallpox to one or more categories of individuals.<sup>29</sup>

Within DHS, the following programs and entities shall be established at the direction of the DHS Secretary:

- an Office for National Laboratories within the Directorate of Science and Technology which shall be responsible for the coordination and utilization of DoE national laboratories and sites in a manner to create a networked laboratory system to support DHS missions;<sup>30</sup>
- a Homeland Security Science and Technology Advisory Committee to make recommendations with respect to the activities of the Under Secretary;<sup>31</sup> and
- the Homeland Security Institute, a federally funded R&D center, which shall: (a) determine the vulnerabilities of the United States' critical infrastructures; (b) assess the costs and benefits of alternative approaches to enhancing security; and (c) evaluate the effectiveness of measures deployed to enhance the security of institutions, facilities, and infrastructure that may be terrorist targets.

With respect to the reliance on the private sector in fulfilling DHS's science and technology objectives, the Secretary is authorized to perform the following specific obligations:

- establish or contract with one or more federally funded research and development centers to provide independent analysis of homeland security issues;<sup>32</sup>
- administer the Homeland Security Advanced Research Projects Agency, including the Acceleration Fund for Research and Development of Homeland Security Technologies,<sup>33</sup> to (a) support basic and applied technology research; (b) advance the development and deployment of critical technologies; and (c) accelerate technologies to prevent existing and future vulnerabilities, in coordination with other "relevant" research agencies;

- establish and promote a program to encourage technological innovation in facilitating the mission of DHS, including creating: (1) a centralized federal clearinghouse to further the dissemination of information on technologies; and (2) a technical assistance team to assist in screening submitted proposals;<sup>34</sup> and
- collaborate with a wide geographic sampling of colleges, universities, private research institutes, and companies to: (a) operate extramural research and development programs; and (b) establish a university-based center or centers for homeland security which shall establish a coordinated, university-based system to enhance U.S. homeland security.<sup>35</sup>

Additionally, the Under Secretary is responsible for: (1) drawing upon the expertise of any government laboratory, including certain DoE national laboratories and sites;<sup>36</sup> and (2) establishing a headquarters laboratory for DHS and additional laboratory units.<sup>37</sup> Except as described above, the Act does not provide specific direction with regard to the disposition of existing federally financed research and development centers, such as those established under the Department of Defense Research Operations.

### Functions Transferred

The Secretary is responsible for developing with HHS a coordinated strategy with respect to civilian human health-related research and development activities relating to countermeasures for chemical, biological, radiological, and nuclear and other emerging terrorist threats.<sup>38</sup> In addition to such coordination efforts, DHS shall also acquire:

- certain DoE functions related to (a) chemical and biological national security programs; (b) nuclear smuggling, detection and assessment programs; (c) biological and environmental research program activities related to microbial pathogens; (d) the Environmental Measurements Laboratory; and (e) the advanced scientific computing research program located at Lawrence Livermore National Laboratory;
- the National Bio-Weapons Defense Analysis Center from the DoD;<sup>39</sup> and
- the Plum Island Animal Disease Center from the Department of Agriculture.<sup>40</sup>

### Title IV—Border and Transportation Security

The Act establishes a new Directorate for Border and Transportation Security and requires the appointment of an Under Secretary of Border and Transportation Security (Asa Hutchinson has been identified as the first such Under Secretary). The Under Secretary of Border and Transportation Security is primarily responsible for:

- preventing the entry of terrorists and the instrument of terrorism into the United States;
- securing the borders, ports, terminals, waterways and any other air, land and sea transportation systems to prevent the entry of terrorists and any instruments of terrorism into the United States;
- administering the customs and immigration and naturalization laws of the United States, including establishing rules governing the granting of visas and other forms of permission to enter the country to individuals who are neither citizens nor lawful permanent residents of the United States;
- establishing national immigration enforcement policies and priorities;
- administering U.S. customs laws (with certain exceptions); and
- ensuring the speedy, orderly and efficient flow of lawful traffic and commerce in fulfilling these responsibilities.<sup>41</sup>

While the Act transfers control over the issuance and denial of visas to the Secretary, the authority to deny visas to aliens on the basis of foreign policy is preserved within the traditional functions of the Secretary of State.<sup>42</sup>

### Functions Transferred

Certain federal agencies and functions related to border and transportation security that are transferred to DHS include:

- the U.S. Customs Service (from the Department of Treasury);
- all Border Patrol, detention and removal, intelligence, investigations and inspections programs within the Immigration and Naturalization Service (from DoJ);
- the Animal and Plant Health Inspection Service (from Department of Agriculture);

- the Coast Guard (from the Department of Transportation (“DoT”));
- the Transportation Security Administration (from DoT);
- the Federal Protective Service of the General Services Administration; and
- the Office for Domestic Preparedness of the Office of Justice Programs (from DoJ).

## **Title V—Emergency Preparedness and Response**

The Act establishes a new Directorate for Emergency Preparedness and Response under the administration of a separate Under Secretary (the announced nominee is Michael Brown, former FEMA Deputy Director and General Counsel). The Under Secretary of Emergency Preparedness and Response must ensure the preparedness of emergency response providers for terrorist attacks, major disasters and other emergencies.<sup>43</sup> Additionally, the Under Secretary must provide the federal government’s response to terrorist attacks and major disasters, including the coordination of the overall response through various formal and informal resources, including: (1) the Domestic Emergency Support Team, (2) the Strategic National Stockpile, (3) the National Disaster Medical System, (4) the Nuclear Incident Response Team, (5) the Metropolitan Medical System, and (6) other federal response resources.<sup>44</sup>

Other responsibilities of the Under Secretary with respect to emergency preparedness and response include:

- aiding in the recovery efforts from terrorist attacks and major disasters;
- working with other federal and non-federal agencies to build a comprehensive national incident management system;
- consolidating existing federal government emergency response plans into a single, unified national response plan;
- developing comprehensive programs for developing interoperative communications technology and ensuring that emergency response providers acquire such technology; and

- establishing standards, training and evaluation procedures and providing funds to support the Nuclear Incident Response Team.<sup>45</sup>

## **Functions Transferred**

In addition to the special direction of the Nuclear Incident Response Team by the Secretary in the event of an actual or threatened terrorist attack, major disaster or other domestic emergency, the Act also transfers to DHS:

- the Federal Emergency Management Agency (FEMA);
- the Integrated Hazard Information System of the National Oceanic and Atmospheric Administration, which shall be renamed FIRESAT;
- the National Domestic Preparedness Office of the FBI;
- the Domestic Emergency Support Teams of DoJ;
- the Office of Emergency Preparedness, the National Disaster Medical System, and the Metropolitan Medical Response System of HHS; and
- the Strategic National Stockpile of HHS.<sup>46</sup>

## **Title VIII—Coordination with Non-Federal Entities; Inspector General; United States Secret Service; General Provisions**

In addition to establishing the primary Directorates, the Act also addresses a range of additional functions and responsibilities for DHS, many of which are new duties within the federal government. Title VIII addresses many of these additional topics.

Within the Office of the Secretary, the Office for State and Local Government coordination will be generally responsible for oversight and coordination with state and local officials and the private sector in advancing the Act’s mission.<sup>47</sup> Such coordination will provide state and local governments with: (a) resource assessments to implement the national anti-terrorism strategy, (b) regular information, research and technical support to assist local homeland security efforts, and (c) a process for providing to the federal government meaningful input regarding the development of the national strategy against terrorism as well as other homeland security activities.<sup>48</sup>

# Homeland Security Bulletin

MARCH 2003

With respect to information sharing activities, within the Act, the Homeland Security Information Sharing Act<sup>49</sup> encourages federal, state, and local entities to share homeland security information to the maximum extent practicable by:

- directing the President to prescribe and implement procedures for federal agency sharing of appropriate homeland security information and handling of classified information and sensitive but unclassified information;<sup>50</sup>
- allowing disclosure to appropriate federal, state, local, or foreign government officials of grand jury matters involving a threat of grave hostile acts of a foreign power, domestic or international sabotage or terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power (threat), within the United States or elsewhere;<sup>51</sup>
- authorizing federal investigative and law enforcement officers conducting communications interception activities, who have obtained knowledge of the contents of any intercepted communication or derivative evidence, to disclose such contents or evidence to: (a) a foreign investigative or law enforcement officer if the disclosure is appropriate to the performance of the official duties of the officer making or receiving the disclosure; and (b) any appropriate federal, state, local, or foreign government official if the contents or evidence reveals such a threat, for the purpose of preventing or responding to such threat;<sup>52</sup> and
- allowing federal officers who conduct electronic surveillance and physical searches in order to acquire foreign intelligence information to consult with state and local law enforcement personnel to coordinate efforts to investigate or protect against such a threat.<sup>53</sup>

With respect to audits or investigations by DHS, or the issuance of subpoenas by DHS, that require access to sensitive information concerning intelligence, counter-intelligence, or counter-terrorism matters, criminal investigations or proceedings, undercover operations, the identity of confidential sources, and certain matters of disclosure, the DHS Inspector General is subject to the authority, direction, and control of the Secretary.<sup>54</sup>

Within the Act, the Support Anti-terrorism by Fostering Effective Technologies Act (“SAFETY Act”) of 2002 authorizes the Secretary to designate and administer protections to anti-terrorism technologies that qualify under a risk management system in accordance with criteria that shall include:

- prior government use or demonstrated substantial utility and effectiveness;
- availability for immediate deployment in public and private settings;
- substantial likelihood that such technology will not be deployed unless protections under such system are extended; and
- the magnitude of risk exposure to the public if such technology is not deployed.<sup>55</sup>

The SAFETY Act further (a) provides a federal cause of action for sellers suffering a loss from qualified anti-terrorism technologies so deployed, (b) prohibits punitive damages from being awarded against a seller, and (c) requires sellers of qualified anti-terrorism technologies to obtain liability insurance in amounts certified as satisfactory by the Secretary.<sup>56</sup>

In furtherance of the stated coordination objectives under Title VIII, within DHS, the Secretary has the following responsibilities:

- appoint a senior DHS official to assume primary responsibility for coordinating policy and operations within DHS and among DHS and other federal departments and agencies with respect to interdicting the entry of illegal drugs into the United States and tracking and severing connections between illegal drug trafficking and terrorism;<sup>57</sup>
- establish within the Office of the Secretary an Office of International Affairs, headed by a Director, to: (a) promote information and education exchange on homeland security best practices and technologies with friendly nations; (b) identify areas for homeland security information and training exchange where the United States has a demonstrated weakness and another friendly nation has a demonstrated expertise; (c) plan and undertake international conferences, exchange programs, and training activities; and (d) manage international activities

within DHS in coordination with other federal officials with responsibility for counter-terrorism matters;<sup>58</sup> and

- establish within the Office of the Secretary the Office of National Capital Region Coordination, headed by a Director, to oversee and coordinate federal homeland security programs for and relationships with state, local, and regional authorities within the National Capital Region.<sup>59</sup>

With respect to other federal agencies, the Secretary must (1) develop an annual federal response plan, which is required to be consistent with public health emergency provisions of the Public Health Service Act and (2) ensure full disclosure of public health emergencies, or potential emergencies, among HHS, DHS, DoJ, and the FBI.<sup>60</sup>

Specific provisions of the Act that directly impact relations with the private sector include the grant of authority to the Secretary to:

- establish, appoint members of, and use the services of advisory committees as necessary;<sup>61</sup>
- engage in transactions, other than contracts, grants and cooperative agreements, for (a) research and development projects for response to existing or emerging terrorist threats; and (b) defense prototype projects, including the employment of private consultants and experts;<sup>62</sup>
- procure property or services to be used to facilitate the defense against or recovery from terrorism or nuclear, biological, chemical or radiological attack;<sup>63</sup> and
- establish a permanent Joint Interagency Homeland Security Task Force, composed of representatives from military and civilian agencies, for the purpose of anticipating terrorist threats and taking actions to prevent harm to the United States.<sup>64</sup>

Additionally, each executive agency shall be required to conduct market research to identify the capabilities of small businesses and new entrants into federal contracting that are available to meet agency requirements in furtherance of defense against, or recovery from, terrorism or nuclear, biological, chemical, or radiological attack.<sup>65</sup> The Act also establishes special streamlined acquisition authority for

a variety of procurements to be conducted by DHS for homeland security-related products and services. These and other related provisions will give DHS great flexibility to contract with technology companies and other contractors on an expedited basis that minimizes the traditional use of certain socioeconomic and pricing contractual provisions.<sup>66</sup>

## Functions Transferred

The Act transfers to the Secretary the functions of the United States Secret Service and the Coast Guard, which both shall be maintained as distinct entities within DHS.<sup>67</sup> Accordingly, the DHS Inspector General shall have oversight responsibility for internal investigations performed by the Office of Internal Affairs of the United States Customs Service and the Office of Inspections of the United States Secret Service.<sup>68</sup>

## Title IX—National Homeland Security Council

The Act establishes within the Executive Office of the President the Homeland Security Council (“Council”) to advise the President on homeland security matters.<sup>69</sup>

Included as members of the Council are: (1) the President; (2) the Vice President; (3) the Secretary; (4) the Attorney General; and (5) the Secretary of Defense.<sup>70</sup> Overall, the Council is required to:

- assess the objectives, commitments, and risks of the United States in the interest of homeland security and make recommendations to the President; and
- oversee and review federal homeland security policies and make policy recommendations to the President.<sup>71</sup>

## Title X—Information Security

Within the Act, the Federal Information Security Management Act of 2002 revises federal government information security requirements.<sup>72</sup> Additionally, the head of each agency operating or exercising control of a national security system must ensure that the respective agency: (1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information; and (2) implements information security policies and practices as required by standards and guidelines for national security systems.<sup>73</sup>

To achieve these objectives, the Act:

- amends the National Institute of Standards and Technology Act to revise and expand the mandate of the National Institute of Standards and Technology to develop standards, guidelines, and associated methods and techniques for information systems; and
- renames the Computer System Security and Privacy Advisory Board as the Information Security and Privacy Board; and requires it to advise the Director of the Office of Management and Budget (“OMB”) (instead of the Secretary of Commerce) on information security and privacy issues pertaining to federal government information systems.<sup>74</sup>

#### Other Functions under the Act

In addition to the major functions summarized above, other Titles of the Act address related homeland security issues, including:

- the overall organization of DHS (Title I);
- the treatment of charitable trusts for members of the U.S. armed forces and other governmental organizations (Title VI);
- management and administration responsibilities of DHS (Title VII);
- establishment and transfer of certain DoJ Divisions (other than the new DoJ Office of Science and Technology), including a new Bureau of Alcohol, Tobacco, Firearms and Explosives (transferred from the Department of Treasury) (Title XI);
- the limitation of liability and extension of insurance policies to airline carriers for third-party claims arising out of terrorist acts (Title XII);
- federal workforce improvements (Title XIII);
- arming pilots against terrorism (Title XIV);
- a reorganization and transition plan under the Act (Title XV);

- certain corrections to existing law relating to airline transportation security (Title XVI); and
- conforming and technical amendments (Title XVII).

#### Effective Dates

The Act became effective on January 24, 2003, 60 days following its enactment, at which time the Bush administration provided to Congress a detailed reorganization plan on the means of administering the creation of DHS. Beginning January 24, 2003, federal officials were given 90 days to oversee and implement the Department’s formation. However, the President stated in the reorganization plan that he anticipates most of the component parts will move into DHS by March 1, 2003. Overall, the Secretary is required to complete the transfer of all 22 federal agencies to DHS no later than January 24, 2004.

#### Additional Information

This summary of the Homeland Security Act has been prepared by members of Kirkpatrick & Lockhart’s Homeland Security practice group. The group includes attorneys in the firm with experience in the areas of government contracting, information security, and government relations, among others. The practice group is assisting clients of the firm with government contract issues arising from the reorganization, as well as questions relating to critical infrastructure information submissions and analyses.

---

*This Bulletin was prepared by  
Jeffrey B. Ritter and Angela Y. Ball.*

For further information regarding the Homeland Security Act, or our law firm’s Homeland Security practice, please contact Robert J. Sherry (rsherry@kl.com; 415.249.1032) or Jeffrey B. Ritter (jritter@kl.com; 202.778.9396).

# Homeland Security Bulletin

MARCH 2003

- 
- 1 See Homeland Security Act of 2002, P.L. 107-296 (Nov. 25, 2002).
  - 2 Id. at § 102(a).
  - 3 Id. at § 101(b).
  - 4 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (“USA PATRIOT Act”) of 2001, P.L. 107-56, §1016(e).
  - 5 See the Act at § 201(d).
  - 6 Id. at § 201(d)(4) (citing 42 U.S.C. 5195c(e)).
  - 7 Id. at § 201(d)(14).
  - 8 Id. at § 201(d)(16).
  - 9 Id. at §§ 201(d)(11), 201(e).
  - 10 Id. at § 202(a).
  - 11 Id. at § 202(b).
  - 12 Id. at § 202(c).
  - 13 See generally §§ 211-215 of the Act.
  - 14 Under Section 212(6) of the Act, “protected system” is defined as “any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure.”
  - 15 See 5 U.S.C. § 552.
  - 16 However, such information may be used or disclosed by any officer or employee of the United States without prior written consent in furtherance of an investigation or the prosecution of a criminal act or to the Comptroller General in performing the duties of the General Accounting Office. Id. at § 214(a)(1).
  - 17 Id. at § 214(e)(1), (f).
  - 18 Id. at § 214(g).
  - 19 Id. at § 221.
  - 20 Id. at § 222.
  - 21 Id. at § 223.
  - 22 Id. at § 224.
  - 23 Id. at § 225.
  - 24 Id. at §§ 231, 232.
  - 25 Id. at § 232(b).
  - 26 Id. at § 234.
  - 27 See generally § 302 of the Act.
  - 28 Id. at § 304.
  - 29 Id. at § 304(c).
  - 30 Id. at § 309(g).
  - 31 Id. at § 311.
  - 32 Id. at § 305.
  - 33 Section 307(c)(2) of the Act authorizes \$500 million in appropriations for the Fund for FY 2003, with such sums “as may be necessary” thereafter.
  - 34 Id. at § 313.
  - 35 Id. at § 308.
  - 36 Id. at § 309.
  - 37 Id.
  - 38 Id. at § 304(a).
  - 39 Id. at §§ 303(1) & (2).
  - 40 Id. at § 310.
  - 41 Id. at § 402.
  - 42 Id. at § 428.
  - 43 Id. at § 502.
  - 44 Id. at § 502(3).
  - 45 Sections 504 and 506 of the Act provide that certain elements of the DoE and the Environmental Protection Agency may be called into service by DHS to form the Nuclear Incident Response Team in connection with an actual or threatened terrorist attack, major disaster or other emergency.
  - 46 Id. at §§ 503, 504.
  - 47 Id. at § 801.
  - 48 Id. at § 801(b).
  - 49 Id. at § 891.
  - 50 Id. at § 892.
  - 51 Such state, local, and foreign officials must use such disclosed information only in conformity with guidelines jointly issued by the Attorney General and the Director of Central Intelligence; Id. at § 895.
  - 52 Id. at §§ 896, 897 (amending 18 U.S.C. § 2517 & 50 U.S.C. § 403-5d).
  - 53 Id. at § 811 (amending 50 U.S.C. § 1806).
  - 54 Id. at § 811.
  - 55 Id. at § 862.
  - 56 Id. at §§ 863, 864.
  - 57 Id. at § 878.
  - 58 Id. at § 879.
  - 59 Id. at § 882.

# Homeland Security Bulletin

MARCH 2003

- 60 Id. at § 887.
- 61 Id. at § 871.
- 62 Id. at §§ 831, 832.
- 63 Id. at § 852.
- 64 Id. at § 885.
- 65 Id. at § 858.
- 66 Id. at §§ 833-35.
- 67 Id. at §§ 821, 888.
- 68 Id. at § 811.
- 69 Id. at § 901.
- 70 Id. at § 903.
- 71 Id. at § 904.
- 72 Id. at § 1001(b) (codified at 44 U.S.C. §§ 3531-3538).
- 73 Id.
- 74 Id. at § 1003.



**Kirkpatrick & Lockhart** LLP

*Challenge us.*<sup>®</sup>

[www.kl.com](http://www.kl.com)

---

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer.

© 2003 KIRKPATRICK & LOCKHART LLP. ALL RIGHTS RESERVED.