

IMPLEMENTATION OF THE HOMELAND SECURITY ACT OF 2002

**PREPARED BY
KELLEY DRYE & WARREN LLP
FOR
USA SECURE**

MARCH 2003

TABLE OF CONTENTS

Page

1.	OVERVIEW	1
1.1	Creation of The New Department of Homeland Security and Effective Date	1
1.2	Mandate and Organization of the Department of Homeland Security	2
1.3	Powers, Practices and Procedures of the New Department	3
1.3.1	Powers and Responsibilities	3
1.3.2	Private Sector Participation.....	7
1.3.3	Role of the Special Assistant To The Secretary.....	9
1.3.4	Limitations on Private Rights of Action	9
1.3.5	Protection of Individual Rights and Liberties.....	9
1.4	Transition	10
2.	DIRECTORATE OF INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION (TITLE II)	10
2.1	Organization.....	10
2.2	Critical Functions.....	11
2.2.1	Designation of Critical Infrastructure and Development of National Plan	11
2.2.2	Information Collection.....	11
2.2.3	Threat Assessment and Warnings.....	11
2.2.4	Information Sharing, Privacy Protection and Security Assurance.....	11
2.2.5	Preventative and Protective Actions	12
2.2.6	Assurance of Cyber Security	12
2.3	Major Issues	13
2.3.1	Designation of Critical Infrastructure	13
2.3.2	Protection of Confidential Information.....	13
2.3.3	Environmental Protection Issues.....	14
3.	DIRECTORATE OF SCIENCE AND TECHNOLOGY (TITLE III)	14
3.1	Organization.....	14
3.2	Critical Functions.....	14
3.2.1	Collaboration with Other Agencies	15
3.2.2	Research, Development, Demonstration, Testing and Evaluation	16

3.2.3	Homeland Security Advanced Research Projects Agency (“HSARPA”).....	16
3.2.4	Homeland Security Science and Technology Advisory Committee.....	16
3.2.5	Homeland Security Institute	17
3.2.6	Technology Clearinghouse to Encourage and Support Innovative Solutions to Enhance Homeland Security.....	17
3.3	Major Issues	17
3.3.1	New Regulations for Contractors.....	17
3.3.2	Funding	17
4.	DIRECTORATE OF BORDER AND TRANSPORTATION SECURITY (TITLE IV).....	18
4.1	Organization.....	18
4.2	Critical Functions.....	18
4.2.1	Assumption and Reorganization of INS Functions	18
4.2.2	Bureau of Border Security	19
4.2.3	Bureau of Citizenship and Immigration Services	19
4.2.4	Office of Domestic Preparedness.....	21
4.3	Major Issues	21
4.3.1	Reorganization of INS Functions.....	21
4.3.2	Coordination of Domestic Preparedness and Emergency Response	21
5.	DIRECTORATE OF EMERGENCY PREPAREDNESS AND RESPONSE (TITLE V).....	21
5.1	Organization.....	21
5.2	Critical Functions.....	22
5.2.1	Establishment of Comprehensive National (Federal, State, Local) Incident Response Plan and Management System.....	22
5.2.2	Acquisition of Technology, Goods and Services for Emergency Response	23
5.3	Major Issues	24
5.3.1	Use of Private Sector Networks	24
5.3.2	Impact on Communications Policy and Providers.....	24
6.	CONCLUSION.....	25

EXECUTIVE SUMMARY

The Homeland Security Act of 2002 (the "Act"), which became effective on January 24, 2003, has set in motion a massive reorganization of the federal government that will result in the establishment of a new Department of Homeland Security with broad and far-reaching powers to wage America's domestic war on terrorism.

The provisions of this law and the powers that will be exercised by the Department are of concern not only to public safety entities and first responders, but to virtually every private sector enterprise that may be affected by a terrorist attack or national emergency. Whether an entity is a public or private sector operator of critical infrastructure, public safety organization, communications or information service provider, manufacturer or industrial concern, other producer of goods and services, government contractor, academic institution or private research and development facility, the implementation of the Act is likely to have a significant impact on the conduct of business.

Implementation of the Act will require attention to an entirely new regulatory authority and compliance with new rules and policies. It will also necessitate new degrees of care and vigilance with respect to the disclosure and dissemination of business information. It may also, however, create significant business opportunities for the provision of goods and services, not only to the Department itself, but to other enterprises that require such goods and services for preparedness and response to terrorism and other national emergencies in compliance with Department requirements.

The new Department is designed to accommodate significant input from the private sector. In fact, a special officer, the Special Assistant to the Secretary, is charged with assessing the impact of Department actions on private industry. In the development of policies and rules, the design of national plans and establishment and evaluation of standards, and the reliance on national networks and private sector goods and services, the Department is required in many ways to operate in significant partnership with, and with substantial sensitivity to, the private sector. Therefore, companies that best understand the complexities of the Department's mandate and functions will be best positioned to protect their interests as well as take advantage of potentially significant commercial opportunities, including funding for technology development.

The attached Advisory provides a summary description of the organization of the new Department, outlines its primary powers and responsibilities, and identifies some of the major issues that will arise in the course of the establishment of the Department's policies, rules and practices. The subject matter is vast and multidisciplinary, and many issues concerning the structure and function of the Department will have to be worked out over the course of many months, if not years. Consequently this Advisory is necessarily preliminary.

Nonetheless, it is clear that the following issues will create high priority concerns that will require substantial attention in the near term:

1. Critical infrastructure protection - determining which assets and operations will qualify as "critical infrastructure" deserving of special protection from terrorist attack, and the practical consequences of such designations.

2. Protection of confidential information - in particular through the establishment of specific rules and procedures regarding the submission, sharing and disclosure of critical infrastructure vulnerabilities, threat assessments and other homeland security information, not only among federal agencies involved in homeland security, but also among state and local authorities as well as certain other private sector enterprises.

3. Interoperability of communications - determining the new policies, standards and lines of jurisdiction that will govern communications systems, both as potential targets of attack and critical resources for public safety and emergency response.

4. Technology development - including the appropriation and grant of funding for research, development, testing and evaluation of security and anti-terrorism technologies. Also, the implementation of streamlined procurement procedures for the use of private sector goods and services by the Department.

5. Immigration - implementation of the reorganization of the Immigration and Naturalization Service which will affect border control and immigration administration.

6. Use of private networks - specifically interpretation of the extent and limitation of provisions in the Act requiring use of private sector networks for emergency response.

7. Environmental issues - including development of eco-security rules regarding the potential environmental impact of terrorist attacks against critical infrastructure and industries.

In our Homeland Security Practice we have assembled a highly qualified, cross disciplinary team headed by James S. Gilmore III, former Governor of the Commonwealth of Virginia and current Chairman of the Congressional Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. We believe that we are uniquely positioned to advise clients in the complex and daunting task of understanding and working with the new Department on homeland security issues. Please let us know if we can assist you. We look forward to your comments and questions.

IMPLEMENTATION OF THE HOMELAND SECURITY ACT OF 2002

James S. Gilmore III, Partner
Chair, Homeland Security Practice Group
Chairman, Congressional Advisory Panel to Assess Domestic Response Capabilities for
Terrorism Involving Weapons of Mass Destruction
Former Governor, Commonwealth of Virginia

Aileen A. Pisciotta, Partner¹

February 2003

1. OVERVIEW

1.1 *Creation of The New Department of Homeland Security and Effective Date*

On November 19, 2002, President George W. Bush signed into law the Homeland Security Act of 2002 (the “Act”), creating a new cabinet-level agency, the Department of Homeland Security (“Department” or “DHS”), designed to coordinate America’s domestic war on terrorism.² The new law became **effective on January 24, 2003**. Former Pennsylvania Governor Tom Ridge, who previously served as the Director of Homeland Security, has been

¹ Contributions to this article also were made by Barton Seitz, partner, and Leila Baheri, Tamara E. Connor, Andrew Klein, Randall Sifers, Richard B. Solomon, Erin Swansiger, associates, of Kelley DRYE & Warren LLP.

² The Homeland Security Act incorporates and/or amends several other statutes, including, for example, the USA PATRIOT Act, the Critical Infrastructure Information Act of 2002, the Cyber Security Enhancement Act of 2002, the Public Health Service Act, the Immigration and Nationality Act, the Robert T. Stafford Disaster Relief and Emergency Assistance Act, the Office of Federal Procurement Policy Act, and Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, the Posse Comitatus Act, the Air Transportation Safety and System Stabilization Act, the Homeland Security Information Sharing Act, the Federal Information Security Management Act of 2002, the National Institute of Standards and Technology Act, the Inspector General Act, the Safe Explosives Act, the Chief Human Capital Officers Act of 2002, the Arming Pilots Against Terrorism Act, the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, and the National Science and Technology Policy, Organization, and Priorities Act of 1976. Numerous sections of the U.S. Code are also amended.

appointed and confirmed as the first Secretary of Homeland Security. Gordon England, currently the Secretary of the Navy, has been appointed as the first Deputy Secretary of Homeland Security.

With approximately 170,000 personnel and a \$40 billion budget for 2003, DHS is required to be largely in place by March 1, 2003 and fully operational within one year. With a broad mandate and sweeping powers, the new Department will have a significant impact on virtually all of our clients. This Advisory provides a preliminary assessment of the new law and issues for the private sector to watch as the Department evolves.

1.2 Mandate and Organization of the Department of Homeland Security

The mandate of the new Department is extremely broad in scope and generally stated. The actual limits and contours of the mandate necessarily will be refined through agency interpretation and action as well as through legal challenge. It encompasses at least the following areas of responsibility:

- (1) Collecting, analyzing, and maintaining databases of intelligence information on terrorist threats and perceived vulnerabilities of the country, particularly involving critical infrastructure, and working with other agencies in the private sector and state and local governments to strengthen U.S. defenses against terror;
- (2) Establishing national plans, strategies and standards, providing the federal response, and coordinating state and local responses to national emergencies, including but not limited to terrorist attacks;
- (3) Serving as a single federal focal point and resource for assistance to state and local entities in combating terror and working with state and local officials to prepare responses to any future national emergencies or terrorist attacks;
- (4) Providing border, coastline and transportation security and administering immigration laws;
- (5) Coordinating efforts to address challenges of nuclear, chemical, biological and cyber terrorism, and encouraging academic and private sector research and development on new technologies that can detect such threats in time to prevent attacks;
- (6) Coordinating the use of private sector technologies, goods and services in homeland security preparations, activities and responses, including developing programs for interoperable communications systems for first responders and homeland security.

Created through a massive reorganization of the federal government involving the transfer of offices and functions from more than 22 existing agencies, including over 100 separate organizations, the new Department is comprised principally of the Office of the Secretary and four Directorates.

The four Directorates, each organized under its own Under Secretary appointed by the President and operating pursuant to a separate title of the Act are:

- Title II Directorate of Information Analysis and Infrastructure Protection
- Title III Directorate of Science and Technology
- Title IV Directorate of Border Transportation and Security
- Title V Directorate of Emergency Preparedness and Response

The Office of the Secretary includes many officers to be designated by presidential appointment. The Deputy Secretary will serve as the first assistant to the Secretary. Up to 12 Assistant Secretaries may be appointed. Additionally, a Special Assistant to the Secretary is charged with creating and fostering strategic communications with the private sector. The President also will appoint other members of the management team, including the Under Secretary for Management, the General Counsel, an Inspector General, a Chief Information Officer, A Chief Human Capital Officer, a Chief Financial Officer and an Officer for Civil Rights and Civil Liberties. Certain distinct entities transferred to or created within the Department also will report directly to the Secretary, including the Secret Service, the Coast Guard, the Office for State and Local Government Coordination, the Office for International Affairs, the Office for National Capital Region Coordination, the Homeland Security Institute, and the Nuclear Incident Response Team.

1.3 Powers, Practices and Procedures of the New Department

1.3.1 Powers and Responsibilities

In the service of its broad mandate, the Department has been given wide ranging powers and responsibilities, some of which are unique to the Department. Many powers are transferred along with agencies and offices, and disentangling the complexities of the rearrangement of powers among the number of offices and agencies involved is likely to take a long time. Several powers and practices granted to the Secretary also are subject to various checks and balances, particularly to ensure the protection of individual rights and liberties. The refinement of the Department's powers and the establishment and evolution of its practices and procedures will directly affect its ability to pursue its mission as well as its impact on the private sector. Thus, it will be critical for the private sector to watch how the Department evolves and to participate where possible in the development process. We have not attempted to provide a complete inventory here of the important powers and practices likely to emerge in the Department, but some of the most important areas to watch include the following:

(i) Regulations

The new Department ultimately will promulgate substantial new rules with significant impact.³ The extent and scope of such potential new rules is not yet clear. Pursuant to Section 877 of the Act, the Secretary is granted only limited new rulemaking powers. These include only the authority to issue regulations concerning “research, development, demonstration, testing, and

³ The Secretary must exercise rulemaking authority in compliance with the Administrative Procedures Act.

evaluation activities of the Department, including the conducting, funding and reviewing of such activities” (Section 306(c)); regulations necessary to implement the Support Anti-Terrorism by Fostering Effective Technologies Act (“SAFETY Act”) of 2002, which, as discussed further below, provides for the designation of anti-terrorism technologies protected from liability (Section 862(c)); and regulations necessary for the protection and administration of federal property in connection with homeland security (Section 1706(b)). In general, however, the Secretary assumes the rulemaking powers held by agencies and offices transferred to the Department. For example, in connection with the abolition of the Immigration and Naturalization Service, the Secretary has authority under Section 428 to issue regulations to administer the Immigration and Nationality Act and related laws.

(ii) Plans, Priorities and Policy-making

Virtually every Directorate is responsible for the recommendation of national plans and policies to address homeland security issues in their areas of jurisdiction. The plans and policies to be developed include a “comprehensive national plan for securing key resources and critical infrastructure” (Section 201(d)(5)); a “national policy and strategic plan for identifying priorities, goals, objectives and policies for...efforts to identify and develop counter measures to chemical, biological, radiological, nuclear and other emerging terrorist threats,” as well as priorities for directing, funding and conducting national research (Sections 302(2) and (5)); “strategic technology development plans” (Section 312(b)(8)); “national immigration enforcement policies and priorities” (Section 402(5)); incorporating strategy priorities into agency planning guidance for agency preparedness for terrorism attacks (Section 430(c)(4)); and creating a “single coordinated national [emergency] response plan” (Section 502(7)). The establishment and implementation of such plans, priorities and policies will have a significant impact with respect to the responsibilities and obligations that may be imposed on the private sector in connection with homeland security.

In many areas, the Secretary is responsible for coordinating among and consulting with a variety of public as well as private sector entities in the establishment and implementation of national plans and policies. Although the Act is clearly intended to foster inter-agency as well as public-private coordination and cooperation, in several areas newly created overlaps may contribute to confusion. For example, the new Office of Science and Technology created in the Department of Justice (Section 231) will focus on law enforcement technologies, but some of the same technologies may fall within the purview of the Department’s Directorate of Science and Technology established under Title III. Similarly, the Department’s Office for Domestic Preparedness created by Section 430 is to be the federal focal point for preparedness for terrorist attacks. However, its duties may overlap with those of the Directorate for Emergency Preparedness and Response established in Title V, which necessarily must be involved in preparedness for response to both terrorist and non-terrorist emergencies. Under Title III, several different organizations are responsible for the promotion and funding of technology developments. Clarifying lines of responsibility in some of these areas will take some time.

(iii) Administration and Program Implementation

A large portion of the Secretary's duties is focused on program implementation and administration. For example, the Secretary will administer rules and program functions in the immigration and border control areas under Title IV. The Secretary also will implement and manage terrorism preparedness and emergency response programs under Titles IV and V. The procedures and practices to be used in fulfilling administrative functions have yet to be determined.

(iv) Adjudication, Investigation and Enforcement

The Secretary has the power to adjudicate visa matters. Pursuant to Section 202(c), the Secretary also is deemed to be a federal law enforcement, intelligence, protective, national defense, immigration or national security official for the purpose of receiving information from law enforcement agencies. In certain arenas, however, the Secretary's enforcement powers are circumscribed. Notably, under Section 101 of the Act, primary responsibility for investigating and prosecuting acts of terrorism remain with federal, state and local law enforcement agencies, except for specific enforcement responsibilities held by agencies transferred to the Department.

(v) Information Gathering and Analysis

One of the primary functions of the Department, particularly in the area of critical infrastructure protection, is the gathering and analysis of information. Information gathered will inform a wide range of the Department's decisions including the assessment of terrorist threats, steps required to protect critical infrastructure and other areas of vulnerability, and the identification of technologies and other products and services deserving of promotion, funding and liability protection. Determinations as to the types of information to be gathered, and the procedures that will govern the acquisition, analysis, storage, manipulation, use, sharing, security and disclosure of information pertaining to homeland security will be among the most closely watched decisions of the new Department. The Act requires that the Secretary establish uniform procedures within 90 days of the enactment of the Act for the "receipt, care and storage" by federal agencies of certain critical infrastructure to be protected from disclosure.

(vi) Promoting Research and Technology Development

The many ways in which the Secretary is directed to promote research and development of homeland security technologies include the following:

Standards-setting

The Secretary is not authorized to set standards for technology to be used by the Department (Section 313(c)(1)). However, acting through the Homeland Security Institute, the Secretary may establish instances when common standards and protocols would improve the effectiveness and interoperability of first responders, and may design test beds and metrics for evaluating the effectiveness of homeland security technologies (Section 312(c)). The Homeland Security Institute is supposed to consult widely with representatives of private industry. The Secretary also is responsible for establishing standards for federal emergency response, particularly acting through the Nuclear Incident Response Team (Section 502(2)).

It should be noted that Subtitle D of Title II (Sections 231-237) of the Act establishes a separate Office of Science and Technology in the Department of Justice to serve as the focal point for the development, testing and evaluation of law enforcement technology. The Office of Science and Technology is responsible for establishing and maintaining performance standards for such technology (Section 231).

Conducting and Promoting Research

Acting primarily through the Directorate of Science and Technology, one of the primary functions of DHS is the promotion of research and development of new technologies that would further the Department's mission. The Act is very clear that, in fulfilling this function, the Directorate of Science and Technology will conduct its own research (Sections 302) and manage research programs (Section 308), but it also must work closely with and foster the efforts both of the private sector and academia.⁴ Through the Homeland Security Institute, the Department also will encourage private sector technological innovation, including through the establishment and maintenance of a clearinghouse of technology information and the provision of technical assistance (Section 313). The conduct of such programs may create significant opportunities for industry.

Funding Technology Development

In combination with the conduct of its own research programs, the Department is empowered to direct funds to third parties for research and development. The Act establishes a special fund, the Acceleration Fund for Research and Development of Homeland Security Technologies (the "Fund"), to be administered by the Homeland Security Advanced Research Projects Agency ("HSARPA") (Section 307). The Fund is to be used for the promotion of revolutionary technologies, as well as the accelerated prototyping and development of technologies to address homeland security vulnerabilities. The procedures by which the HSARPA will set priorities, invite proposals, conduct competitive bids for grants and otherwise administer the Fund have yet to be determined.

Separately, the Secretary, acting through the Under Secretary for Science and Technology, will distribute funds through grants, cooperative agreements and contracts through "Extramural Programs" involving academia and the private sector, and "Intramural Programs" with other government agencies, to conduct basic and applied research, development, testing and evaluation activities relevant to the responsibilities of the Department (Section 308). The issuance of regulations governing the conduct of such research and development activities, particularly funding, should be carefully watched.

Providing Anti-Terrorism Risk Protection

Under the SAFETY Act (Title VIII, Subtitle G, Sections 861-865), the Secretary will be able to afford risk protection to designated anti-terrorism technologies. Such protection involves provisions regarding insurance, the creation of a defined federal cause of action for damages

⁴ Section 308(b)(2) requires that within one year of the date of enactment of the Act, the Secretary establish a university-based center or centers for homeland security.

resulting from acts of terrorism when qualified technologies have been used, and limitations on damages that may be recovered by plaintiffs. As mentioned above, the rules that will govern qualifications for such risk protection are yet to be developed.

(vii) Streamlined Contracting for Commercial Goods and Services

The Act requires in several places that the Department promote the participation of the private sector in homeland security activities. In particular, the Secretary must rely to the “maximum extent practicable” on the use of private sector networks and infrastructure for emergency response (Section 508). It is not clear what terms and conditions will govern such use. The Secretary also should avoid competing with the private sector by relying on commercially available technologies, goods and services for the needs of the Department (Section 509).

The Act includes several provisions that aim to facilitate and streamline the ability of private industry to contract with the Department for technologies, goods and services. For example, Subtitle D of Title VIII (Sections 831-35) includes provisions for procurement of temporary and intermittent expert or consulting services in cases of “urgent homeland security need,” and streamlined acquisition authority in cases where, in writing, the Secretary determines that the mission of the Department would be “seriously impaired” without the use of such authorities. Section 834 requires that, within one year of the enactment of the Act, the Federal Acquisition Regulations (“FAR”) be revised to include regulations regarding the evaluation of unsolicited proposals. Subtitle F of Title VIII (Sections 851-58) also provide for federal emergency procurement flexibility for one year from the date of enactment of the Act by an executive agency as required to “facilitate defense against or recovery from terrorism or nuclear, biological, chemical, or radiological attack.” Additionally, Section 858 requires that heads of executive agencies affirmatively seek out new entrants and small businesses as contractors to meet anti-terrorism requirements.

Notably, Section 835 prohibits contracts with “corporate expatriates,” which are companies or partnerships with substantial U.S. business or assets that are incorporated or organized abroad to avoid tax or other fiduciary duties in the U.S.

(viii) Reports to Congress

The Act requires that the Secretary and numerous other government officials report periodically to different Congressional committees on various activities, resource inventories, program implementation developments and status, compliance plans, public impact, and legislative requirements. Tracking of such reports will provide critical insight into the way the Departments policies, procedures and practices are taking shape.

1.3.2 *Private Sector Participation*

In several respects, the Act creates the incentive and opportunity for the private sector to actively participate, and even partner with the new Department, in activities addressing homeland security concerns. Such participation may take many different forms, and the nature and extent of such opportunities will only be known after the Department becomes operational.

However, the statute expressly provides that, in addition to the input that may be provided to the Special Assistant to the Secretary, private sector companies and individuals also may:

(i) Consult with the Under Secretary for Information Analysis and Infrastructure Protection on the appropriate exchanges of law enforcement information (Section 201(d)(11)); and with the Homeland Security Institute, established to perform systems and risk analysis, economic and policy analysis, technical evaluation and metrics design and security-related exercises and simulations (Section 312(c) and (d));

(ii) Serve as analysts of critical infrastructure information (Section 201(e)(2));

(iii) Request technical assistance from the Department with respect to emergency recovery plans to respond to major failures of critical information systems (Section 223(2));

(iv) Volunteer to participate in the “NET Guard” to be established to provide scientific and technological expertise to assist local communities to respond to and recover from attacks on information systems and communication networks (Section 224);

(v) Compete for grants from the Acceleration Fund for Research and Development of Homeland Security Technologies (\$500 million to be appropriated in 2003) to be administered by the Director of the HSARPA. Grants are to be made available for research, development, testing, evaluation and prototyping of technologies addressing homeland security issues (Sections 307(b)(3) and (c)). As described above, other research and development grants also may be available through the Directorate of Science and Technology’s “Extramural Programs” (Section 308(b));

(vi) Enter into agreements for cooperative research and development or licenses with a Department of Energy national laboratory utilized by the Secretary of Homeland Security (Section 309(d));

(vii) Participate in advisory committees to be established by the Secretary (see generally Section 871), such as the Technology Advisory Committee to assist in the development of an Internet-based system to permit individuals and employers to gain online access to information regarding the processing status of immigration-related applications (Section 461(c));

(viii) Provide off-the-shelf commercially developed information technologies and other goods and services for use by the Department in the conduct of its business (Section 509);

(ix) Benefit from the use of streamlined procurement procedures for property or services used to “facilitate defense against or recovery from terrorism or nuclear, biological, chemical, or radiological attack,” especially new entrants and small businesses. (Sections 852, 856, and 858); or

(x) Obtain a Certificate of Conformance, as well as a listing on the Secretary's Approved Product List for Homeland Security, for the sale of anti-terrorism technology that qualifies for risk protection under the SAFETY Act (Sections 861-65).

1.3.3 Role of the Special Assistant to the Secretary

Section 102(f) establishes the position of Special Assistant to the Secretary. This key individual will serve as an essential interface between the Department and the private sector. He or she will serve as the focal point for input on the impact of Department policies and regulations on the private sector, as well as the key advisor, if not decision-maker, on private sector projects, partnerships and practices to address homeland security issues.

The Special Assistant will have broad discretion to create mechanisms for "strategic communications" between the Department and the private sector, including the creation of private sector advisory councils to advise the Secretary on such issues as private sector solutions to homeland security challenges. The Special Assistant also is charged with working with the private sector to develop technologies for homeland security missions, promoting public-private sector partnerships and assisting in the development of private sector best practices to secure critical infrastructure. Clearly, the development and evolution of the role of the Special Assistant to the Secretary, as well as the establishment, function and opportunities for participation in private sector advisory councils, will have a substantial effect on the nature and extent of impact of the new Department on the private sector, as well as on new opportunities for businesses in the homeland security arena.

1.3.4 Limitations on Private Rights of Action

Several provisions of the Act constrain private rights of action. Section 215 specifies that no private right of action is created by any provision of Title II Subtitle B (providing for the protection of the confidentiality of voluntarily provided critical infrastructure information) for enforcement of any provision of the Act. Section 428(f) provides that there is no private right of action to challenge a decision of a consular officer or other U.S. official or employee to grant or deny a visa. Subtitle G of Title VIII pertaining to the SAFETY Act limits actions for recovery for damages from sellers of protected anti-terrorism technologies.

1.3.5 Protection of Individual Rights and Liberties

The Act, however, does establish several officers charged with protecting individual rights and liberties. Section 222 requires that the Secretary appoint a Privacy Officer to ensure compliance of the Department with the Privacy Act and that the use of technologies by the Department does not erode privacy protections for personal information. Section 452 establishes the position of a Citizenship and Immigration Services Ombudsman, reporting to the Deputy Secretary, to assist individuals in resolving any problems with, and recommending improvements in the responsiveness of, the Bureau of Citizenship and Immigration Services. Section 705 also requires the Secretary to appoint an Officer for Civil Rights and Civil Liberties who is responsible for "reviewing and assessing information alleging abuses of civil rights, civil liberties, and racial and ethnic profiling by employees and officials of the Department."

1.4 Transition

The Office of the Secretary was established as of January 24, 2003. Also as of that date, many of the offices should be effective, including several within the Secretary's Office, as well as the Bureau of Border Security, the Bureau of Citizenship and Immigration and the Director of Shared Services, who is responsible for the coordination of information resources for the Bureau of Border Security and Bureau of Citizenship and Immigration Services.

Certain federal agencies will be abolished as a result of the Act, with the functions, assets and liabilities of such entities transferred to various entities within the Department and elsewhere (*e.g.* the Immigration and Naturalization Service). In other instances, only certain portions or duties of the federal agency will be transferred to the Department (*e.g.* the United States Coast Guard), and in still other instances, an agency will continue to exist as a distinct entity within the Department (*e.g.*, the United States Secret Service.) The transfers are not supposed to affect either the completed administrative actions of the pending proceedings of a transferred agency. All agency transfers are expected to be substantially complete by March 1, 2003, with the exception of the Plum Island Animal Disease Center of USDA, which will not be transferred until June 1, 2003. Also as of June 1, 2003, the Homeland Security Science and Technology Advisory Committee is expected to be established. All incidental transfers of personnel, assets and liabilities of various entities to be transferred to the Department should be completed by September 1, 2003.

2. DIRECTORATE OF INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION (TITLE II)

2.1 Organization

The Directorate of Information Analysis and Infrastructure Protection will be created through the transfer by March 1, 2003 of five agencies into the Department: the National Infrastructure Protection Center of the FBI (other than the Computer Investigations and Operations Section), the National Communications System of the Department of Defense, the Critical Infrastructure Assurance Office ("CIAO") of the Department of Commerce, the National Infrastructure Simulation and Analysis Center of the Department of Energy, and the Federal Computer Incident Response Center ("FedCIRC") of the General Services Administration. Other personnel from the State Department, Central Intelligence Agency ("CIA"), Federal Bureau of Investigation ("FBI"), National Security Agency ("NSA"), National Imagery and Mapping Agency, and the Defense Intelligence Agency are to be detailed to the Department to assist with analytic and related functions.

2.2 Critical Functions

The critical functions of the Directorate of Information Analysis and Infrastructure Protection are as follows:

2.2.1 *Designation of Critical Infrastructure and Development of National Plan*

The Under Secretary for Information Analysis and Critical Infrastructure must develop a comprehensive national plan for securing key resources and critical infrastructures, including power production, generation, and distribution systems, information technology and transmission systems, and emergency preparedness communication systems. Section 213 of the Act authorizes the President or the Secretary to determine which functions within the new Department should be designated as critical infrastructure programs entitled to receive information regarding the vulnerabilities and protection of critical infrastructure.

2.2.2 *Information Collection*

Section 202 of the Act entitles the Secretary to receive certain intelligence and other information from all federal agencies for analysis in service of the Department's mandate to protect critical infrastructure. The Secretary may enter into cooperative arrangements with other agencies regarding such information, and specifically is required to consult with the Director of the CIA and other agencies to establish collection priorities and strategies for information related to terrorist threats. The Secretary must establish and secure communications and information infrastructure to use in the collection and analysis of relevant information, including data mining and advanced analytical tools.

2.2.3 *Threat Assessment and Warnings*

Utilizing the information collected, the Secretary must assess current and future threats to key resources and critical infrastructures and issue timely warnings through the administration of the Homeland Security Advisory System.

2.2.4 *Information Sharing, Privacy Protection and Security Assurance*

The Act imposes an affirmative obligation on all federal agencies to furnish the Secretary with all information concerning terrorist threats and infrastructure vulnerabilities. The Secretary is required to ensure that its databases and analytical tools are compatible with those of other federal agencies, assessing threats and issuing warnings, and sharing information "as appropriate" with other federal, state and local authorities. The Secretary is required to ensure that material received by the Department is used only for the performance of official duties and is protected from unauthorized disclosure. Section 221 requires the Secretary to establish procedures to ensure the security of information obtained and to protect the statutory and constitutional rights of subject individuals.

Subtitle I of Title VIII (Sections 891-99) also establishes the Homeland Security Information Sharing Act, pursuant to which the President is to prescribe and implement procedures for the sharing of "relevant and appropriate" homeland security information among

federal agencies and with “appropriate State and local personnel,” which may include “private-sector entities that affect critical infrastructure, cyber, economic, or public health security, as designated by the Federal Government in procedures developed pursuant to this section” (Section 892(f)(3)(F)). Thus, private industry should be concerned not only with the sharing of homeland security-related information among federal agencies, but also among state and local authorities as well as other private sector entities.

2.2.5 Preventative and Protective Actions

In addition to issuing warnings of terrorist threats, the Under Secretary is responsible for “immediately taking or effecting” appropriate preventative and protective actions. The Act does not clearly specify permissible means for generally meeting this responsibility.

2.2.6 Assurance of Cyber Security

The Act places substantial emphasis on cyber security. Section 223 requires that the Secretary provide to state and local governments, and upon request to private sector entities that own or operate critical information systems, analysis and warnings related to threats and vulnerabilities of critical information systems. To protect against cyber attacks, Section 224 of the Act permits the Under Secretary to create a national corps of volunteers with expertise in science and technology to “assist local communities to respond and recover from attacks on information systems and communication networks.”

Further, Section 225 of the Act incorporates the entire text of the Cyber Security Enhancement Act (CSEA), which was previously approved by the full House. The CSEA directs the United States Sentencing Commission to review its guidelines applicable to certain computer crimes and submit a report to Congress, by May 1, 2003, of actions taken. The Act allows Internet service providers (“ISPs”) to voluntarily provide government agents with access to the contents of customer communications without consent based on a “good faith” belief that an emergency justifies the release. This is intended to ease fear of lawsuits on the part of ISPs due to information sharing with law enforcement. The Act also specifies that an existing ban on the “advertisement” of any device that is used primarily for surreptitious electronic surveillance applies to online ads. It introduces fines and 20-year prison terms for offenders who “knowingly” or “recklessly” cause or attempt to cause serious bodily injury and provides up to life sentence for computer intrusions that “knowingly” or “recklessly” put others’ lives at risk. It permits limited surveillance without a court order, including the installation of pen register and trap and trace devices, when there is an “ongoing attack” on a “protected computer”⁵ or “an immediate threat to a national security interest.” Surveillance is limited to obtaining a suspect’s telephone number, Internet address or email header information – not the contents of online communications or telephone calls.

⁵ As defined, any computer involved in interstate commerce or communications qualifies as a “protected computer.”

2.3 Major Issues

2.3.1 *Designation of Critical Infrastructure*

It is unclear what facilities will actually be designated as critical infrastructure. The Act references Section 1016 of the USA PATRIOT Act, which in turn defines “critical infrastructure” as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”⁶ The definition is certainly open to interpretation. The transfer of such offices as CIAO and the National Infrastructure Simulation and Analysis Center to the Department puts the interpretation of the USA PATRIOT Act provisions under the Secretary’s jurisdiction. Thus, as a practical matter, the determination of what constitutes critical infrastructure will fall to the Secretary.

2.3.2 *Protection of Confidential Information*

The protection of information regarding critical infrastructure and vulnerabilities to terrorist attack is of paramount concern, particularly as the Act provides for the widespread dissemination of homeland security information among federal, state and local authorities as well as the private sector.

To address these concerns, Section 214 provides that information voluntarily provided by non-federal parties to the Department that relates to the security of critical infrastructure or protected systems shall be exempt from disclosure under Section 552 of the Freedom of Information Act (“FOIA”), when accompanied by an express statement specified in the Act. Such information should not lose its protected character if forwarded by the Department to other federal agencies. Moreover, information voluntarily provided is not subject to rules concerning *ex parte* communications and may not be used in any civil action if such information has been submitted in good faith. The provisions of this section pre-empt state law to insure that the information is not disclosed by state openness laws. The Act provides for punishment, including fines and imprisonment for up to one year, of any Department employee for disclosing any voluntarily submitted critical infrastructure information that is not customarily in the public domain.

The extent of the protection actually accorded by this provision is as yet uncertain. The Homeland Security Act does not expressly amend FOIA, and the application of the statutory definition of “voluntary” may be subject to interpretation. Procedures for the receipt and storage of critical infrastructure information are to be established within 90 days of the enactment of the Act. However, there is no deadline for the establishment by the President of the new procedures required under Section 892 for sharing of homeland security information with “appropriate State and local personnel,” although a progress report must be submitted to Congress within one year.

⁶ The text of the USA PATRIOT Act also expressly includes “cyber infrastructure, telecommunications infrastructure, and physical infrastructure” as critical infrastructure.

2.3.3 *Environmental Protection Issues*

One of the critical areas that the new Homeland Security Department may seek to address through regulations are eco-security programs to protect against harm to people and/or the environment from the possible release of hazardous materials due to terrorist or other criminal attacks against nuclear and other electric power plants, petroleum and natural gas pipelines, chemical manufacturing and storage facilities and other industrial facilities. Such protective programs are not expressly required under the Act, but the need for eco-security programs for critical infrastructure likely will be examined in the context of the Department's threat assessment analysis. Any regulatory proposals regarding eco-security for critical infrastructure would raise a number of serious questions, such as which facilities should be encouraged or required to implement these programs, whether security measures should be federally-mandated or only voluntarily implemented, and whether facility assessments and other business information relating to security evaluations would be legally protected from disclosure.

3. DIRECTORATE OF SCIENCE AND TECHNOLOGY (TITLE III)

3.1 Organization

The Science and Technology Directorate also will be created through the transfer of programs and activities from other agencies. Some programs include those formerly within the Department of Energy, including chemical and biological national security and supporting programs and activities of the nonproliferation and verification research and development program; the nuclear smuggling and assessment programs and activities; life sciences activities of the biological and environmental research program related to microbial pathogens; the Environmental Measurements Laboratory; and the advanced scientific computing research program and activities at Lawrence Livermore National Laboratory. The Department of Defense National Bio-Weapons Defense Analysis Center, including related functions of the Secretary of Defense, also will be transferred.

3.2 Critical Functions

The Directorate of Science and Technology generally will be responsible for research and development efforts in support of homeland security, including: identifying and developing countermeasures to chemical, biological, radiological, nuclear, and other emerging terrorist threats; assessing and testing vulnerabilities and possible threats; establishing priorities for, directing, funding, and conducting research, developing, testing and evaluating, and procuring technology and systems to prevent the importation of chemical, biological, radiological, nuclear, and related weapons and material; and detecting, preventing, protecting against, and responding to terrorist attacks.

The Act establishes the following primary areas of responsibility in support of the Department's science and technology agenda:

3.2.1 *Collaboration with Other Agencies*

The Under Secretary is responsible for coordinating with other executive agencies in carrying out the Department's science and technology agenda. The Act specifies that, among others, the Department will collaborate with the Department of Agriculture, the Department of Health and Human Services, and the Department of Energy.

(i) Department of Agriculture

The Under Secretary will collaborate with the Secretary of Agriculture and the Attorney General on a variety of topics, including the transfer of responsibility for the Plum Island Animal Disease Center to the Secretary of Homeland Security. The Department of Agriculture will be allowed continued access to the Center, and the Secretary of Agriculture will continue to direct Department of Agriculture research, diagnostic, and related activities at the Center.

(ii) Department of Health and Human Services

Cooperation between agencies will be necessary for the conduct of certain public health-related activities. To that end, the Department will collaborate with the Secretary of Health and Human Services and the Attorney General to determine any new biological agents and toxins. The Secretary also will have the authority to issue a declaration concluding that an actual or potential bioterrorist incident or other public health emergency makes administration of a "covered countermeasure" (e.g., smallpox vaccine) to a category or categories of individuals advisable; each declaration must be promptly published in the Federal Register. The Act further limits the liability of the United States in such a situation.

(iii) Department of Energy

The Act provides for establishment of an Office for National Laboratories. The Office will be responsible for coordination and utilization of the Department of Energy national laboratories and sites to create a networked laboratory system for purposes of supporting the Department. The Under Secretary will enter into work agreements and other arrangements with the Department of Energy for use of its many national laboratories and sites. The Act provides that the Department may use Department of Energy national laboratories through a variety of methods provided by law, and may be a joint sponsor of a Department of Energy national laboratory or site, with the Secretary of Energy acting as lead agent.

These work agreements must comply with the policy of federally funded research and development centers under the Federal Acquisition Regulations. Furthermore, the Department will be required to provide funds under a joint sponsorship arrangement under the same terms and conditions that apply to the primary sponsor under federal law. All direct contracts with operators of national laboratories and Department of Energy sites must be kept separate from the direct contracts between the Department of Energy and the site operator. Likewise, cooperative research and development agreements and licensing agreements, as well as technology transfers to non-federal parties, must be consistent with appropriate federal law.

3.2.2 Research, Development, Demonstration, Testing and Evaluation

The primary science and technology mission of the Act – research, development, demonstration, testing and evaluation – will be carried out through a combination of “extramural” and “intramural” programs. Extramural programs, including university-based centers for homeland security and programs with the private sector, are to be established within one year of the date of enactment. Criteria for selection will include demonstrated expertise in relevant areas such as: food safety; emergency medical services; chemical, biological, radiological and nuclear countermeasures; port and waterway security; having a nationally recognized program in information security; and strong affiliations with diagnostic laboratories, among other factors.

The Department will be allowed to draw on the expertise of any laboratory of the federal government, whether operated by a contractor or the government itself. A Department headquarters laboratory and additional laboratory units may be established at any laboratory or site. Furthermore, the Under Secretary may establish or contract with federally funded research and development centers to provide independent analysis of homeland security issues or to carry out other responsibilities under the Act.

3.2.3 Homeland Security Advanced Research Projects Agency (“HSARPA”)

The Director of HSARPA, who will report to the Under Secretary, will administer the Acceleration Fund for Research and Development of Homeland Security Technologies, award competitive grants and contracts to public and private entities, and support accelerated research, testing, and deployment of critical homeland security technologies to promote homeland security and address vulnerabilities. HSARPA also will coordinate with other research agencies, and possibly operate joint projects. Personnel will be appointed for a maximum of five years.

For fiscal year 2003, \$500 million has been appropriated for the Fund. At least ten percent of funds for each year through fiscal year 2005 are to be set aside for the Coast Guard for research and development of improved ports, waterways and coastal security surveillance.

3.2.4 Homeland Security Science and Technology Advisory Committee

The Under Secretary will appoint 20 members to the Advisory Committee, which will make recommendations and identify research areas of potential importance to national security. The Advisory Committee will include emergency first responders and representatives of organizations or associations of emergency first responders, and citizen group representatives, and will provide representation of a cross-section of the research, development, demonstration, and deployment activities being supported by the Under Secretary.

Members will be appointed to three year terms, and the original appointments will be made in three classes of three members each with staggered terms. The Committee will also establish rules for determining whether a member has a conflict of interest in a matter before it.

3.2.5 *Homeland Security Institute*

The Institute will be a federally funded research and development center, administered as a separate entity by the Secretary. Its operations will be determined by the Secretary, and may include systems analysis, risk analysis, simulation and modeling to determine vulnerabilities, provide economic and policy analysis, design and support for conduct of homeland security-related exercises and simulations, and creation of strategic technology development plans to reduce vulnerabilities in the critical infrastructure. The Institute will consult widely with private and public entities.

3.2.6 *Technology Clearinghouse to Encourage and Support Innovative Solutions to Enhance Homeland Security*

The Technology Clearinghouse is intended to encourage technological innovation in service of the mission of the Department, and will include the following five components: a centralized federal clearinghouse relating to technologies that would further the mission of the Department; issuance of announcements seeking unique and innovative technologies; establishment of a technical assistance team to assess the merits of proposals; provision of guidance to other government agencies and private sector efforts to evaluate and implement the technologies; and provision of information for persons seeking guidance on how to develop or deploy such technologies. However, the Clearinghouse will not set standards for technology to be used by the Department.

3.3 Major Issues

3.3.1 *New Regulations for Contractors*

It would not be surprising to see a number of new rules and regulations result from the creation of this division. The Under Secretary will have the authority to issue new regulations with respect to research, development, demonstration, testing and evaluation activities of the Department, including conducting, funding, and reviewing of such activities. In this respect, implementation of the Act should provide a number of contracting opportunities for private organizations. However, companies contracting with federal agencies pursuant to the Act also will face new regulations and compliance requirements.

3.3.2 *Funding*

Although Title III contemplates the funding of various “extramural programs” for research, development, demonstration, evaluation and testing of homeland security technologies, including by private sector entities, the Act does not expressly authorize appropriations for such funding. Consequently the amount, nature and terms and conditions of any such funding are unclear.

4. DIRECTORATE OF BORDER AND TRANSPORTATION SECURITY (TITLE IV)

4.1 Organization

The Directorate of Border and Transportation Security will be constituted from the transferred functions of a number of existing federal agencies and offices. Chief among these is the INS which is abolished under Section 471 of the Act, and largely replaced by the new Border and Transportation Security Directorate.⁷ Other offices to be transferred to the Directorate include the United States Customs Service of the Department of Treasury (except customs revenue functions, such as assessing and collecting customs duties, which will not transfer); the Transportation Security Administration (“TSA”) of the Department of Transportation; the Federal Protective Service (“FPS”) of the General Services Administration; the Federal Law Enforcement Training Center (“FLETC”) of the Department of the Treasury; and the Office for Domestic Preparedness of the Office of Justice Programs. Certain agricultural inspection functions of the Secretary of Agriculture also will be transferred.

4.2 Critical Functions

The Secretary, acting through the Under Secretary for Border and Transportation Security, is responsible for preventing the entry of terrorists and instruments of terrorism into the United States; securing the borders and transportation systems; carrying out immigration enforcement functions; establishing and administering rules governing the granting of visas, or other forms of permission, for non-citizens to enter the United States; and establishing national immigration enforcement policies and priorities.

4.2.1 *Assumption and Reorganization of INS Functions*

The Directorate is to include two separate bureaus created from the INS: one governing border security, and the other governing citizenship and immigration services. The Act prohibits the Secretary from using the reorganization authority given to him to recombine the two immigration bureaus into a single agency, or otherwise combine, join or consolidate functions or units of the two bureaus with each other. It does, however, permit the reorganization of the functions within each bureau. The Act creates the position of Director of Shared Services within the Office of Deputy Secretary, responsible for the coordination of resources for the two immigration bureaus, including: information resources management; records and file management; and forms management. The Act further establishes separate accounts in the U.S. Treasury for the two immigration bureaus. Budget requests for each bureau are to be submitted separately. Fees for services, applications or benefits are to be deposited into the account of the bureau that has jurisdiction over the function to which the fee relates. Unlike the INS, where service and enforcement budgets were co-mingled, the Act specifically states that fees are not transferable for purposes that are not set forth with §286 of the Immigration and Nationality Act.

⁷

Jurisdiction over a few matters are transferred from the INS to other agencies; for example, issues regarding unaccompanied alien children are transferred to the Office of Refugee Resettlement of the Department of Health and Human Services.

The reorganization of the immigration agency into separate enforcement and service bureaus may allow for more efficient processing of immigration petitions and applications. Previously, user fees collected by the INS paid by those seeking immigration benefits accounted for the majority of the agency's budget. However, the fees collected went into a general INS account which were used to pay for the enforcement as well as service budgets. Due to pressures to provide additional security at the nation's borders and ports of entry, funds that were earmarked for the service staff were often allocated towards enforcement, causing delays in the service side of the agency. The separation of the budgets for enforcement and service and the prohibition of commingling funds should allow the bureau to hire and retain sufficient staff to improve processing times.

4.2.2 *Bureau of Border Security*

The Bureau of Border Security will be headed by an Assistant Secretary, who will report directly to the Under Secretary for Border Security. The Assistant Secretary will control and establish policy for the Border Patrol program, as well as the detention and removal program, the intelligence program, the investigations program, and the inspections program. Among other things, the Assistant Secretary is charged with establishing policies and overseeing the administration of the immigration functions and administering the Student and Exchange Visitor Information System and other programs established to collect information relating to foreign students and other exchange program participants.

The Act creates two additional positions within the Bureau of Border Security. A Chief of Policy and Strategy is responsible for consulting with personnel in local offices; researching policy issues; analyzing and making policy recommendations on immigration enforcement issues; and coordinating immigration policy with Chief of Policy and Strategy for the Bureau of Citizenship and Immigration. The Legal Advisor provides legal advice to the Assistant Secretary for Border Security and will represent the Bureau in all exclusion, deportation, and removal proceedings before the Executive Office for Immigration Review ("EOIR").⁸

4.2.3 *Bureau of Citizenship and Immigration Services*

(i) Responsibilities of the Director

The Bureau of Citizenship and Immigration Services will be headed by a Director who will report directly to the Deputy Secretary. The Director will be charged with advising the Deputy Secretary with respect to any policy or operation of the Bureau that may affect the Bureau of Border Security and establishing national immigration services policies and priorities. The Director will have authority for several functions previously administered by the Commissioner of the INS, all adjudications previously performed by the INS including adjudications of immigrant visa petitions, naturalization petitions, asylum and refugee applications, and adjudications performed at service centers.

⁸ EOIR remains a separate agency within the Department of Justice, under the authority of the Attorney General.

(ii) Citizenship and Immigration Services Ombudsman

A Citizenship and Immigration Services Ombudsman will serve to identify problem areas between individuals or employers and the Citizenship and Immigration Bureau, to assist with resolution of such problems and to propose changes to mitigate future such problems. The Ombudsman will submit written recommendations to the Director of the Citizenship and Immigration Services Bureau with respect to all administrative actions necessary to resolve problems encountered by individuals and employers, to which the Director must formally respond.

(iii) Issuance of Visas

Prior to the enactment of the Act, authority over the issuance of visas rested exclusively within the province of the State Department and the Secretary of State. The Act now vests in the Secretary of Homeland Security (acting through the Secretary of State) exclusive authority to administer and enforce all laws, and to issue regulations relating to the functions of consular officers in the granting or refusal of visas, including the authority to develop programs of homeland security training for consular officers.⁹

While granting authority over administration and enforcement of laws related to visa issuance, the Act does not give the Secretary of Homeland Security the authority to alter or reverse the decision of a consular officer to refuse a visa. The Act does, however, authorize the Secretary of State to direct a consular officer to refuse a visa to an alien if the Secretary of State deems such refusal necessary or advisable in the foreign policy or security interests of the United States. In addition, the Secretary of State continues to retain authority under certain areas of the Immigration and Nationality Act. It remains to be seen how effectively the State Department and the Department of Homeland Security will be able to work on joint matters that had been the exclusive province of the State Department, especially with respect to the oversight of Department of Homeland Security employees over consular officials.

The Secretary of Homeland Security is authorized to assign employees of the Department of Homeland Security to each diplomatic and consular post at which visas are issued, unless it is determined that such an assignment would not promote homeland security. Employees of the Department who are assigned to diplomatic or consular posts will provide advice and training regarding security threats relating to the adjudication of individual visa applications or classes of applications, will review any such applications, and will conduct investigations with respect to consular matters under the jurisdiction of the Secretary of Homeland Security.

⁹ This section will take effect either when the President publishes notice in the Federal Register that Congress has received the memorandum of understanding between the Secretary and the Secretary of State governing implementation of this section, or one year after the enactment of the Act, whichever comes first.

4.2.4 *Office of Domestic Preparedness*

The Directorate for Border and Transportation Security also contains the Office of Domestic Preparedness, headed by a Director who also reports directly to the Deputy Secretary of the Department. This Office bears the primary responsibility within the Executive Branch for preparing the United States for acts of terrorism and for coordinating preparedness efforts at all levels in all matters pertaining to combating terrorism on behalf of the United States.

4.3 Major Issues

4.3.1 *Reorganization of INS Functions*

The Act requires an extensive overhaul of functions previously performed by the INS, which is abolished by Section 471. There undoubtedly will be challenges and problems with the implementation of these changes, which includes the separation of border control and immigration issues into two separate bureaus. There could also be significant “turf” battles and policy clashes between and among the officers charged with implementing this reorganization, including the Under Secretary for Border and Transportation, the Assistant Secretary of the Bureau of Border Security (who reports to the Under Secretary), the Director of the Bureau of Citizenship and Immigration (who reports to the Deputy Secretary and not the Under Secretary and is to advise the Deputy Secretary of any potentially conflicting policies or operations with the Bureau of Border Security), the Ombudsman (who reports to the Deputy Secretary), the Director of Shared Services (who also reports to the Deputy Secretary and who is charged under Section 475 with overseeing the sharing of information resources, databases, records and forms between the two bureaus), and the Department of State.

4.3.2 *Coordination of Domestic Preparedness and Emergency Response*

The Office for Domestic Preparedness, located within the Directorate of Border and Transportation Security, must closely coordinate with the agencies that comprise the Directorate of Emergency Preparedness and Response. The Act specifies that the Office of Domestic Preparedness is to focus on federal preparedness for acts of terrorism, and is supposed to coordinate closely with FEMA, which is located in the Bureau of Emergency Preparedness and Response and has primary responsibility for non-terrorist disasters. However, the fact that domestic preparedness for acts of terrorism is the responsibility of the Under Secretary for Border Transportation and Security while the emergency response, including for acts of terrorism, is the responsibility of the Under Secretary for Emergency Preparedness and Response, may create unnecessary overlap and confusion.

5. DIRECTORATE OF EMERGENCY PREPAREDNESS AND RESPONSE (TITLE V)

5.1 Organization

Section 501 of the Act establishes a Directorate of Emergency Preparedness and Response under the authority of an Under Secretary. Agencies and functions related to emergency preparedness transferred to the new Directorate include: (1) FEMA; (2) the Integrated

Hazard Information System of the National Oceanic and Atmospheric Administration, which will be renamed “FIRESAT;” (3) the national Domestic Preparedness Office of the FBI, including related functions of the Attorney General; (4) the Domestic Emergency Support Teams of the Department of Justice, including the related functions of the Attorney General; (5) the Office of Emergency Preparedness, the National Disaster Medical System, and the Metropolitan Medical Response System of the Department of Health and Human Services including the related functions of the Secretary of Health and Human Services and the Assistant Secretary for Public Health Emergency Preparedness, and the Strategic National Stockpile of the Department of Health and Human Services, including the related functions of the Secretary of Health and Human Services.

Functioning as separate and distinct entities assisting in emergency preparation and response, yet under the direct authority of the Secretary, are the Nuclear Incident Response Team, which is activated in cases of actual or threatened terrorist attack, the United States Secret Service, and the Homeland Security Institute, a federally funded research and development center, whose duties may include systems/risk analyses to determine vulnerabilities in the nation’s critical infrastructures, and assessment of alternative approaches to enhancing security.

5.2 Critical Functions

The Directorate is charged with aiding to ensure the effectiveness of emergency response providers to terrorist attacks, major disasters, and other emergencies. The critical functions of the Directorate of Emergency Preparedness and Response are as follows:

5.2.1 *Establishment of Comprehensive National (Federal, State, Local) Incident Response Plan and Management System*

(i) Coordination With Department of Health and Human Services

Under Section 505 of the Act, the Secretary must coordinate emergency relief efforts with the Department of Health and Human Services. With respect to all public health-related activities to improve state, local, and hospital preparedness and response to chemical, biological, radiological, nuclear, and other emerging terrorist threats carried out by Health and Human Services, the Secretary of that Department must set priorities and preparedness goals and develop a coordinated strategy for these activities with the Secretary of Homeland Security. The Secretary of Health and Human Services must collaborate with the Secretary of Homeland Security in setting benchmarks and outcome measurements for evaluating the progress towards achieving the goals of their agencies’ coordinated strategy.

(ii) Federal Emergency Management Agency (“FEMA”)

Subject to the provisions of the Act, the FEMA retains all of the functions and authority originally granted to it by the Robert T. Stafford Disaster Relief and Emergency Assistance Act, and maintains its status as the lead agency for the Federal Response Plan. Within 60 days of the enactment of the Act, the Director of FEMA must revise the Federal Response Plan to incorporate the Department and reflect the establishment of this entity. The Act requires that FEMA pursue its mission to reduce the loss of life and property and protect the Nation from all hazards by leading and supporting the Nation in a comprehensive, risk-based emergency

management program. The Act identifies five main points upon which the program should be based: (1) mitigation, by taking sustained actions to reduce or eliminate long-term risk to people and property from hazards and their effects; (2) planning for building the emergency management profession to prepare effectively for, mitigate against, respond to, and recover from any hazard; (3) response, by conducting emergency operations to save lives and property through positioning emergency equipment and supplies, evacuating potential victims, providing food, water, shelter, and medical care to those in need, and restoring critical public services; (4) recovery, by rebuilding communities so that individuals, businesses, and governments can function on their own, return to normal life, and protect against future hazards; and (5) increased efficiencies, by coordinating efforts relating to mitigation, planning, response and recovery.

(iii) Nuclear Incident Response Team

Under Section 504 of the Act, the Directorate is responsible for setting standards, conducting joint exercises and training, evaluating performance and providing funds to the Department of Energy (“DOE”) and the Environmental Protection Agency (“EPA”) in relation to the Nuclear Incident Response Team.¹⁰ In instances of actual or threatened terrorist attacks, major disasters, or other emergencies in the United States, the Secretary has the authority to call into service the Nuclear Incident Response Team. During this time only, the Nuclear Incident Response Team shall operate under the direction, authority and control of the Secretary. This grant of authority to the Directorate does not limit the ordinary responsibility of the Secretary of Energy and the Administrator of the EPA for organizing, training, equipping and utilizing their respective entities in the Nuclear Incident Response Team, or from exercising direction, authority and control over them when they are not operating as a unit of the Department.

5.2.2 Acquisition of Technology, Goods and Services for Emergency Response

Section 509 of the Act may potentially benefit the private sector and create a new market for existing technology. Specifically, it requires the Secretary, to the extent possible, to use off-the-shelf commercially developed technologies. The Secretary must use such technology to ensure that the Department’s information systems allow the Department to collect, manage, share, analyze and disseminate information securely over multiple channels of communications. Furthermore, in order to avoid competition with the private sector, the Secretary should rely on commercial sources to supply the goods and services needed by the Department. This is in line with existing Federal policies to avoid commercial competition with the private sector.

¹⁰ Section 506 states that for purposes of Title V of the Act, The Nuclear Incident Response Team is made up of entities from the DOE and the Environmental Protection Agency. It includes those entities of the DOE that perform nuclear or radiological emergency support functions, radiation exposure functions at the Radiation Emergency Assistance Center/Training Site (“REAC/TS”), radiological assistance functions, and related functions. From the EPA, it includes those entities that perform such support functions, including radiological emergency response functions, and related functions.

5.3 Major Issues

5.3.1 *Use of Private Sector Networks*

Section 508 requires that the Secretary use national private sector networks and infrastructure, to the extent practicable, for emergency response to chemical, biological, radiological, nuclear, or explosive disasters, and other major disasters. This section does not define the term “national private sector networks and infrastructure” and sets no parameters for the prescribed use. The terms and conditions of the use of such networks are not addressed, and it is not clear whether the Act contemplates or permits the appropriation of private sector networks and infrastructure in the event of such emergencies. It is further unclear if the use may occur only in times of emergency and major disasters, i.e. a temporary take over of the infrastructure and networks, or if arguably, the Department should use these private facilities in their everyday operations in preparation for response to such emergencies and disasters, or the requirements and obligations that may be imposed on private networks and infrastructure to ensure that they may be serviceable to the Department in the event of an emergency. The extraordinary breadth and vagueness of this provision raises significant concerns and will require close monitoring of its implementation.

5.3.2 *Impact on Communications Policy and Providers*

Several provisions of the Act have potential significance for the establishment of communications policy and the operation of communications networks by public as well as private sector entities. Section 502(7) requires that the Under Secretary for Emergency Preparedness and Response develop “comprehensive programs for developing interoperative communications technology, and helping to ensure that emergency response providers acquire such technology.” Pursuant to a related provision, Section 223, the Under Secretary for Emergency Preparedness is expected to coordinate with the Under Secretary for Information Analysis and Infrastructure Protection to provide analysis, warnings, crisis management support and technical assistance to state and local entities, as well as to private sector upon request, to assist in response to threats or attacks on “critical information systems.” Under Section 201 the Under Secretary for Information Analysis and Infrastructure is charged directly with developing a national plan for securing telecommunications systems that constitute critical infrastructure. Meanwhile, the Office of Science and Technology established in the Department of Justice is charged in Section 232(b)(7) with administering “a program of research, development, testing, and demonstration to improve the interoperability of voice and data public safety communications. Finally, pursuant to Section 430, the Office of Domestic Preparedness in the Directorate of Border and Transportation Security has primary responsibility within the executive branch for “coordinating or, as appropriate, consolidating communications and systems of communications relating to homeland security at all levels of government.”

These provisions raise a number of significant questions. As an initial matter, they are very broadly written and lack any definitions of the terms “communications technology,” “communications systems,” “critical information systems,” and interoperability.” Conceivably the provisions apply to all manner of communications technologies and systems, regardless of the technology employed (i.e., wireline or wireless) and without distinction between private commercial systems, private non-commercial (e.g., utility) systems, and public sector systems

(e.g., municipal or other government and public safety). The authority of various officials of the Department of Homeland Security and/or the Department of Justice to mandate technologies, standards, protocols or procedures for response to threats or attacks, to achieve “interoperability,” or to ensure availability for Department use in the event of an emergency is completely unclear.

The diffusion of responsibility for these issues promises to create confusion at best, and direct conflicts at worst, in the obligations, expectations and standards imposed on communications systems by various homeland security officials. Significant conflict may also arise between the Department of Homeland Security and other communications authorities, including the Federal Communications Commission and the Department of Commerce’s National Telecommunications and Information Administration. This is particularly true with respect to spectrum allocation and utilization for critical infrastructure and public safety, but also with respect to network reliability and cyber security. The availability of spectrum, avoidance of interference and standards for interoperable use for any and all communications systems that may need to be used in a national emergency will present a complex set of issues with many masters that will have to be carefully navigated over the coming months.

6. CONCLUSION

The implementation of the Homeland Security Act raises a myriad of complex concerns for the private sector. Over the coming months, new homeland security procedures and policies will be established across a broad range of substantive areas with significant impact on nearly every sector of the economy. While it is impossible at this early stage to forecast all of the issues that may arise, we believe that the following issues are deserving of high priority attention:

1. Designations and policies regarding the protection of “critical infrastructure.”
2. Rules and procedures regarding the submission, sharing and disclosure of critical infrastructure vulnerabilities, threat assessments and other homeland security information.
3. Development of new policies, standards and lines of jurisdiction governing communications systems, both as potential targets of attack and critical resources for emergency response.
4. Implementation of technology programs, including funding for research and development, streamlined procurement procedures and designation of protected anti-terrorism technologies.
5. Implementation of the INS reorganization.
6. Interpretation of provisions requiring use of private sector networks for emergency response.
7. Development of eco-security rules regarding the potential environmental impact of terrorist attacks against critical infrastructure and industrial targets.