Homeland Security Bill Holds New Opportunities for Technology Companies

2002-12-30

The Homeland Security Act of 2002, which President Bush signed into law on November 25, 2002, has been described as a massive consolidation of 22 federal agencies and approximately 170,000 employees with a wide range of anti-terrorism responsibilities.

Beyond the new organizational charts, however, the Homeland Security Act contains numerous provisions of interest to private-sector technology companies, including stronger cyber-security measures, authorizations for targeted public-private research initiatives, sales opportunities for commercial technology products and services, streamlined procurement policies, and limitations on legal liabilities. Through these provisions, the new Department of Homeland Security (DHS) is expected to leverage "private sector products, applications and solutions as they relate to homeland security challenges." See our November 14, 2001 Internet Alert on the Defense Department's previous effort to solicit commercial solutions following the terrorist attacks of September 11, 2001.

Technology Infrastructure and Cyber-Security Enhancements

The DHS Directorate for Information Analysis and Infrastructure Protection will collect and analyze homeland security information and intelligence and protect the nation's government and private-sector critical information technology networks.

In order to encourage non-federal entities to provide DHS with information about threats to critical computer systems, information voluntarily provided to DHS may be protected from use for other purposes and can be provided under an exemption from disclosure under the Freedom of Information Act. Recognizing that non-government networks are vulnerable to terrorist attacks, the law directs DHS to provide analysis, warnings, crisis management, and technical assistance to private-sector operators of critical information systems and proposes the creation of a "NET Guard" corps of volunteer technical experts to assist local authorities to respond and recover from cyber-attacks.

The law instructs DHS to utilize commercial technologies and service providers to improve the government's domestic intelligence-gathering capabilities. A DHS Privacy Officer will be responsible for monitoring these information collection technologies, reviewing DHS regulations, and reporting

to Congress on DHS efforts to protect individual privacy.

The law also adds new protections against unauthorized access to information networks. Among these provisions are increased penalties for cyber-terrorism under the Computer Fraud and Abuse Act and a prohibition of Internet advertising of devices that illegally intercept electronic communications.

Federally-Supported Acquisitions, Research & Development

Given its size and complex mission, the new DHS may quickly become a major consumer of commercial products and services, including significant purchases of commercial information technologies and software. So far, however, a widely expected wave of new homeland security contracts has been slow to materialize. This is due in part to a moratorium on major information technology acquisitions by DHS component agencies, imposed by the White House in July 2002 to avoid redundant acquisitions while DHS needs are assessed. In addition, DHS will have to compete for funding with other federal budget priorities, because the law authorizes, but does not fund, new homeland security initiatives.

However, as the consolidated agency's acquisition requirements are defined, new opportunities for technology companies will emerge. For example:

- The new Bureau of Citizenship and Immigration Services (a successor to the current Immigration and Naturalization Service) is directed to seek "Internet-based technologies" for providing information and receiving filings affecting millions of immigrants.
- DHS and other federal agencies are required to implement information security safeguards "commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction" of the data maintained on agency systems, and the law states a preference for commercial information security solutions.

The DHS Directorate of Science and Technology will be a new focus for public-private collaboration on technologies addressing chemical, biological, radiological, nuclear, and other terrorist threats. The law provides for a wide range of homeland security R&D initiatives, including:

- A Homeland Security Advanced Research Projects Agency to provide competitive awards to private companies to develop priority technologies, supported by a proposed "Acceleration Fund" of up to $500 million, subject to Congressional funding.
- Homeland security-related collaborations with the Department of Energy's renowned national laboratories, which already provide funding, research facilities, and technical expertise to private companies.
- Coordination of human health research projects conducted by the Department of Health and Human Services, which houses the National Institutes of Health and the Centers for Disease Control and Prevention.
- A DHS advisory commission, a research institute and a technology clearinghouse, intended to promote private-sector participation in DHS science and technology activities.

In addition, the law creates a new Justice Department Office of Science and Technology to fund R&D projects in areas such as monitoring and alarms, communications systems, and DNA identification.

Streamlined Procurement Rules

The Homeland Security Act contains streamlined procurement policies that may be a model for future changes in government-wide acquisition policies. Among the special rules for DHS acquisitions are expanded authorizations to make noncompetitive purchases, increased thresholds for using “simplified” procurement methods, and broader use of “commercial” contract terms. Other federal agencies will be permitted to use these streamlined procedures for emergency acquisitions related to homeland security needs.

The law helps companies with innovative technologies by requiring federal agencies to make ongoing efforts to identify “new entrants” that may be able to provide anti-terrorism products or services to the government.

New Liability Limitations

The law provides new protection for companies that disclose electronic communications to law enforcement agencies. Specifically, the law amends the Electronic Communications Privacy Act, 18 USC 2702(b), to permit electronic communication providers to disclose the contents of a subscriber’s message in emergency situations involving a danger of death or personal injury.

Other provisions limit the legal liability of companies that are sued for alleged defects in vaccines and certain anti-terrorism technologies. For technology suppliers, these protections include a prohibition on punitive damages, limitations on noneconomic damages, and an extension of the so-called “government contractor defense” that shields companies from liability for work performed under federal direction.

The new DHS will immediately become one of the largest federal government entities, with perhaps the most complex set of missions. In creating DHS, Congress acknowledged the critical role of commercial technology companies in protecting homeland security and in providing the tools needed to operate the vast new Department. The Homeland Security Act provides a blueprint for involving the technology sector in homeland security.

Authors

Barry J. Hurewitz

PARTNER

barry.hurewitz@wilmerhale.com

+1 202 663 6089