# Technology Companies Boosted by Government Anti-Terrorist Purchases

2001-11-14

United States federal and state government agencies are planning major purchases from technology companies in order to bolster homeland security and to support the war against terrorism. As a result, the anti-terrorism effort is generating opportunities for technology companies in an otherwise gloomy economy.

The federal government is already the nation's largest consumer of technology products and services. Anti-terrorism initiatives will add to the government's technology needs, resulting in new acquisitions as well as the acceleration or expansion of procurements that were already planned.

Homeland security is expected to require significant information technology investments to protect critical federal government systems and to build new systems for preventing and responding to terrorist attacks. Federal officials have recently likened the homeland security effort to the government's multi-billion dollar mobilization to address the Year 2000 computer problem. As an indication of the size of the problem, U.S. airport commissioners have estimated that it may cost up to $4 billion simply to enhance airport security, through means such as biometric passenger screening, physical security improvements, and improved baggage screening.

The Defense Department – the largest federal purchasing organization – is aggressively seeking technology companies with practical, new ideas for fighting terrorism in the U.S. and abroad. The Pentagon especially hopes to attract innovative proposals from leading-edge companies that have no experience in government contracting. Participation is unusually easy – only a one-page concept proposal must be submitted by December 23, 2001. Those submitting the most promising concepts will be invited to negotiate more detailed project proposals. The Defense Department is seeking proposals in the following technical areas:

**Technologies for Combating Terrorism**

- language and voice recognition
- computer and information operations
- tagging, tracking, locating and remote sensors
- locating faces in video images

- identifying faces in video images
- video human tracking
- voice print identification
- terrorist behavior and actions predictions technologies
- information integration
- physical security of personnel, equipment and facilities
- ports of entry passenger screening (rapid deception detection)
- advanced distributed learning

**Technologies for Locating and Defeating Hard or Difficult Targets**

- detection and mapping of underground facilities
- tactical operations support

**Technologies for Protracted Operations in Remote Locations**

- early warning devices (detection of non-friendly forces)
- direct action (improvements in information, weapons and armor)
- specialty munitions
- advanced optical and thermal tactical imaging systems
- advanced breaching tools (entry of masonry and metal structures)
- through-wall imaging technologies

**Countermeasures to Weapons of Mass Destruction**

- identifying terrorists involved with or handling weapons of mass destruction
- entry point screening for explosives, chemicals and radiological weapons
- chemical, biological, radiological and nuclear countermeasures
- pre-release detection of chemical and biological agents
- air sampler and aerosol collection
- remote sensors for predicting the source of a weapon of mass destruction
- neutralizing chemical and biological agents
- field testing kits for biological analysis
- database for assessment of materials used in weapons of mass destruction
- explosives detection (standoff detection and handheld detectors)
- walkthrough portals for personnel screening (metal detection and imaging)
- technologies for defeating terrorist devices
- standoff large vehicle bomb diagnostics
- large vehicle bomb neutralization, containment and mitigation
- tools for disposal of explosives

Simultaneously, the federal government has increased its spending on bioterrorism preparedness programs, and even more funding is being considered. Several agencies led by the Department of Health and Human Services have intensified their efforts to develop and stockpile vaccines and antibiotics, largely through contracts with pharmaceutical and biotechnology companies and providers of related technologies and services. The Bush Administration has requested an additional $1.5 billion for bioterrorism preparedness, most of which would be set aside for vaccine and antibiotic testing and production. Congressional leaders from both parties have proposed similar increases.

Other changes in federal agencies’ technology acquisitions are more subtle. Several agencies with national security functions have already increased orders under existing agreements. Agencies will also be less likely to delay – or may accelerate – planned information technology systems upgrades. In fact, federal budget officials have specifically promised to "protect" information technology spending proposals from the scrutiny that will be imposed for other post-September 11 funding requests.

Following the principle that "all terrorism is local, "state and local governments across the country are also rushing to develop or improve plans to prepare critical computer systems, public infrastructure, and the health care system for terrorist attacks. So far, these efforts have included new plans for Internet-based monitoring of critical systems, tracking of communicable diseases, improving the real-time data available to law enforcement agencies, and improving the exchange of information among different jurisdictions.

Disturbed by reported vulnerabilities in critical government computer systems, Congress is expected to approve additional federal spending that will benefit technology companies. An organization of the government’s leading information technology vendors predicts that federal government information technology acquisitions will rise by some 15% over the next year. One proposal currently before Congress would create a billion-dollar information technology fund, to be used for major IT projects intended to strengthen and safeguard important government information systems.

Although many of the details remain to be worked out, the anti-terrorism effort will require the public sector to rely more than ever before on the products and services of technology companies.

## *Authors*

**Barry J. Hurewitz**

PARTNER

✉ barry.hurewitz@wilmerhale.com

☎ +1 202 663 6089

Wilmer Cutler Pickering Hale and Dorr LLP is a Delaware limited liability partnership. WilmerHale principal law offices: 60 State Street, Boston, Massachusetts 02109, +1 617 526 6000; 2100 Pennsylvania Avenue, NW, Washington, DC 20037, +1 202 663 6000. Our United Kingdom office is operated under a separate Delaware limited liability partnership of solicitors and registered foreign lawyers authorized and regulated by the Solicitors Regulation Authority (SRA No. 287488). Our professional rules can be found at www.sra.org.uk/solicitors/code-of-conduct.page. A list of partners and their professional qualifications is available for inspection at our UK office. In Beijing, we are registered to operate as a Foreign Law Firm Representative Office. This material is for general informational purposes only and does not represent our advice as to any particular set of facts; nor does it represent any undertaking to keep recipients advised of all legal developments. Prior results do not guarantee a similar outcome.