

## **Technology in Homeland Security: A Double-Edged Sword**

**Hosted by the  
George Washington University's Homeland Security Policy Institute  
and the  
IBM Global Leadership Initiative**

**9 June 2008**

Technology holds forth the promise of solving a host of our greatest homeland security and counterterrorism challenges by providing the right information to the right people at the right time. Technology also represents an abiding challenge when projects fall short of promises, privacy protections are subordinated to other goals, and men and women on the front lines are left frustrated by new technologies that complicate their jobs before making them easier.

As part of ongoing efforts to build bridges between theory and practice, The George Washington University Homeland Security Policy Institute (HSPI) joined with the IBM Global Leadership Initiative to co-host a panel discussion on technology issues in homeland security on June 9, 2008. IBM's Global Leadership Initiative is an innovator for IBM's Global Business Services that identifies critical public sector challenges, convenes expertise from a variety of disciplines, and develops thought leadership to address a broad range of issues to solve complex problems in the public sector.

The panel examined successes and failures from both the public and private sectors to draw lessons crucial to the success of future homeland security investments and innovation. Key factors discussed by the panel and described below include:

- Proactive privacy protections,
- Governance designed with the private sector and user community in mind,
- Human capital development,
- Agile requirements design for a range of users, and
- Fostering technology innovation from all parts of the market.

The following represents a distillation of the themes and observations that emerged from the panel presentations, as well as the roundtable discussion that followed with the more than seventy participants from the public sector, industry, non-profit, and international communities.

# Technology in Homeland Security: A Double-Edged Sword

## ~Speaker List~

### **Parney Albright**

Managing Director and Vice Chairman  
of Civitas, LLC  
Former Assistant Secretary of Homeland  
Security for Science and Technology,

### **Christian Beckner**

Professional Staff Member, US Senate  
Homeland Security and Governmental  
Affairs Committee

### **Bradley Buswell, Keynote Speaker**

Deputy Under Secretary of Homeland  
Security for Science and Technology

### **Frank Cilluffo**

Director, Homeland Security Policy  
Institute

### **Jonah Czerwinski**

Senior Fellow for Homeland Security,  
IBM Global Leadership Initiative

### **Langdon Greenhalgh**

CEO, Global Emergency Group

### **Jan Lane**

Deputy Director, Homeland Security  
Policy Institute

### **Greg Nojeim**

Director, Project on Freedom, Security  
and Technology at the Center for  
Democracy and Technology

## Highlights

### I. Serving the Technology Needs of a Highly Diverse Market

The Department of Homeland Security's Directorate for Science and Technology (S&T) serves stakeholders from local sheriffs to the commanders of NORTHCOM and everything in between. The diversity of and divisions within this market greatly compound S&T's task of meeting the technology needs of the country's homeland security personnel. The Department of Homeland Security (Department) contains 22 different agencies, each with often very different technology needs. Moreover, some of those agencies, such as the Transportation Security Administration, are recent creations, while others, such as the Coast Guard, have existed for over two hundred years, significantly differentiating the management processes involved for each.

Even within agencies there can be segmented markets. For example, within Customs and Border Protection, Customs officials naturally have very different needs and goals than do Border Patrol agents. Beyond the Department is the patchwork of state and local jurisdictions, each of which oversees an array of law enforcement entities, fire departments, and other agencies relevant to the homeland security mission. These are all customers with specific technology

needs, and, even where requirements overlap, there are many barriers to the sharing of best practices across the market. Department of Homeland Security S&T is managing a customer-driven technology development process to address this challenge.

## **II. Designing Customer-Driven Technologies**

S&T has worked to overcome the hurdle of a diverse market in part by enabling the customers themselves to drive the technology development and acquisition process as much as possible as part of a "customer-driven" process. This process depends upon twelve Capstone Integrated Product Teams (IPTs), each dedicated to a functional area of homeland security:

- border security,
- cargo security,
- chemical/biological defense,
- cyber security,
- transportation security,
- countering improvised explosive devices,
- incident management,
- information sharing,
- infrastructure protection,
- interoperability,
- maritime security, and
- people screening.

Each IPT consists of S&T's customers and critical stakeholders, such as state and local law enforcement, fire departments, emergency medical services, private sector partners, and quasi-public entities like airports. Through IPTs, S&T can better identify high priority technology needs and capability gaps by working directly with end-users. S&T has also set up the TechSolutions Project, through which first responders and field agents can contact S&T directly via the Web to report desired technologies. In this way, front-line personnel can engage S&T directly, thereby streamlining the process of meeting requirements.

There is still work to be done, and S&T could learn from the way the private sector develops products for their customers. Some firms, for example, co-locate teams with customers for months, studying in detail the ways they use technologies – illustrating one way that S&T could expand its customer-driven processes.

## **III. Requirements Setting for Department of Homeland Security Partners**

Working directly with customers will not alone solve the problem of matching technologies to homeland security agencies and first responders. Customers can articulate technology needs and capability gaps but often lack the ability to assess the technologies that might meet those needs. A city police chief, looking for radiation detectors for squad cars, might receive thirty or forty proposals – and

with no expertise in radiation detection technology, would have no way of independently evaluating the proposals. The Department faces the same problem on a much larger scale. Most homeland security technology on the market is being developed by small businesses selling in local markets. The Department lacks the funds and personnel to evaluate every proposal it receives, much less every technology in the market. Requirements setting will be one of the most important tasks S&T can undertake for its customers.

Homeland Security S&T seeks to develop requirements against which homeland security technologies can be evaluated. Setting, updating, and disseminating these requirements will be a key role of S&T in promoting technology development and acquisition across the country. A knowledge database, providing benchmarks against which customers can measure technologies and highlighting technologies that meet specific needs, will be invaluable to the Department's state, local, and commercial partners.

#### **IV. Developing Context-Specific Technologies**

Requirements setting, rather than just disseminating technologies, is important not just as a cost- and time-saving measure, but because individual customers often have diverging needs based on context. In the US, homeland security personnel might seek ways to use increasingly ubiquitous social networking websites for promoting emergency preparedness and awareness. In contrast, halfway around the world in a disaster zone, emergency responders might face a devastated infrastructure and lack even basic communications equipment, requiring an immediate deployment of satellite phone technology. Using cell phones to transfer money and inject cash into communities might be much more effective in Africa, with its well-developed cell networks, than in South Asia, where cell phone use is less common. From arming unmanned aerial vehicles with anti-missile systems to protecting airports, to using GIS mapping systems to identify populations affected by an emergency, to deploying inflatable barriers to plug breached levies temporarily, S&T's partners often have unique needs that cannot be met by a standard set of technologies. Rather than evaluating every potential technology for each of these markets, S&T will best serve many of these customers by setting requirements in each area that can empower customers to make informed evaluations on their own.

#### **V. Developing Homeland Security Technologies before Threats Materialize**

S&T does not solely rely on input from customers to begin development of homeland security technologies. Since many technologies take years to develop, waiting for intelligence warnings of a threat or for customers to place requests could leave responders empty handed when a threat does materialize. Improved

explosive devices (IEDs), for example, are cheap and easy to make. Many, usually in the forms of pipe bombs, are set off each year in the US, though there is no indication that they will be used in the US in a coordinated campaign against infrastructure and soft targets any time soon. Nevertheless, the capability for such a campaign is already in place – and motivation is a constantly shifting factor. Having technologies in the development pipeline could ensure that adequate responses are available if and when a threat like an IED campaign does appear. In preparation for this possibility, S&T is seeking to develop not just detection and mitigation technologies, but also the fledgling fields of hostile intent identification and the psychology of terrorism.

Panelists and participants agreed that there is a risk that this could become a costly “anything’s possible” approach. Trying to prepare for every imaginable threat would quickly bankrupt the homeland security enterprise. Instead, S&T must prioritize development on an ongoing basis by using intelligence reports and such strategic guidance as the National Strategy for Homeland Security and other White House directives. S&T also prioritizes those threats that may be neutralized through existing technology, such as IEDs or certain cyber attacks. In addition, the office conducts scenario planning with a range of other agencies to identify likely future threats and corresponding gaps in capability.

## **VI. Protecting Privacy and Keeping the Public’s Trust**

Public trust is the key to success for many homeland security initiatives. Though it takes long to establish trust, it can be eroded quickly. From the unauthorized mining of private data to the highly publicized difficulties in getting Senator Ted Kennedy’s name off the TSA No Fly List, the Department has faced a number of challenges in winning and maintaining the public’s trust and confidence in its deployment of new technologies.

Many promising technologies have foundered or are foundering in the absence of public trust, especially with regards to privacy concerns. The Real ID program, which requires state drivers licenses to meet national standards and provide interoperable data tracking, met resistance from varying constituencies due to a lack of restrictions on how businesses could access the information. Funding for the Total Information Awareness program, initiated by the Department of Defense after 9/11, was cut after the public protested its goal of processing huge amounts of financial, travel, and other data. (Rather than being a privacy victory, this was actually a privacy setback as the TIA program was moved from the Department of Defense to another agency with less transparency and public oversight.) Mission creep is another concern, as anti-terrorism technologies pique the interest of law enforcement officers looking to use them to identify outstanding warrants or immigration violation. Concerns over how data will be used, shared, stored, and

secured have disrupted the development and deployment of homeland security technologies.

The Department is working to improve public perceptions of its work and homeland security technologies. Senior officials are working to promote awareness of the importance of public trust and confidence among their staffs. Earning the public's trust demands that homeland security technologies are developed with privacy protections "built in" at the start of development process, not added on in response to criticism or privacy concerns.

This will be a challenge to law makers as much as to the Department. In many cases, the law has failed to keep pace with technological developments. Case law, for example, indicates that there are no privacy rights with regard to records held by third-parties such as banks and phone companies. Over time, however, these organizations have come to acquire huge amounts of data on citizens. The law has not kept pace with these changes, raising the possibility of vast data mining with little oversight. Cell phones can generate information about a person's location – and law enforcement wants the right to access this information. The law, written before cell phones existed, does not adequately address this issue. Technologies that protect or enhance privacy are dependent on privacy rights enshrined in law, requiring action on the part of lawmakers to update laws and keep pace with technological developments.

## **VII. Moving Forward**

Despite failures along the way, both the U.S. government and the private sector are now attempting to consider these challenges carefully. Shortly before this panel event took place, the Department of Homeland Security held its annual S&T Stakeholders conference in Washington, DC, at which over 600 participants from the private sector and Homeland Security S&T community were in attendance. This annual conference is an outlet for the factors described above to be integrated into S&T efforts. In the ensuing weeks, the U.S. Senate passed a rewrite of the 1978 Foreign Intelligence Surveillance Act, or FISA, to overhaul disputed rules on secret government eavesdropping, demonstrating progress on yet unresolved policy and privacy concerns. Policymakers and the private sector should continue to press momentum forward.