

The Four Main Challenges of the Department of Homeland Security

By Ed Badolato, Executive Vice President for Homeland Security, The Shaw Group

On January 24, 2003 the law creating the US Department of Homeland Security came into effect, and its first Secretary, Thomas J. Ridge was sworn in. This was the most extensive reorganization of the Federal Government since the 1940s when President Harry Truman reorganized the Nation's fragmented military defenses to help win the Cold War. The purpose of the DHS was to fuse the current confusing patchwork of government activities into a single department with the mission of securing our homeland. The strategy of the new department is threefold: to prevent terrorist attacks within the US; to reduce America's vulnerability to terrorism; and to minimize the damage and recover from attacks that do occur

The DHS has four main challenges in the following areas: crafting an effective corporate organization; developing a capability to effectively gather terrorism information and distribute intelligence; obtaining adequate funding; and meeting the new legal issues of the post 9/11 environment.

First among DHS' organizational challenges are the requirements to address the line management concerns and the resistance to change that could be found in any new organization, especially one as diverse, huge, and complex as the DHS.

In addition to the management problems associated with organizing the DHS' overall structure from 22 separate agencies, is the challenge of resistance to change. One of Secretary Ridge's top priorities will be to merge the cultures of the former 22 agencies into one gigantic, seamless department. But there will be difficulties in creating more direct lines of authority and allaying cultural concerns about uniforms, shoulder patches and long standing procedures.

The management difficulties involved in building effective intra organizational communications systems—both classified and unclassified—will be tremendous. Coordinating the purchase and use of computers, cell phones, PDAs, etc, throughout a DHS workforce of approximately 170,000 will be daunting task.

The next DHS challenge involves the overall topic of intelligence. Foremost in this area are the problems of upgrading the capability of the intelligence community to combat terrorism and decreasing the competition between the FBI and the CIA.

The 9/11 attacks were the intelligence communities most serious failure since Pearl Harbor, but it is unlikely that any serious reforms will take place. In December 2002 a joint congressional committee made 19 recommendations, with little effect. An independent commission on 9/11 intelligence headed by former NJ governor Thomas Kean is not scheduled to deliver its report until 2004. The mastermind of the 9/11 attacks, Khalid Sheikh Mohammed, was recently arrested in Pakistan, but he was well known as a key Al Qaeda official by the US intelligence committee as early as 1996

because of his role in a plot to sabotage US airliners over the Pacific and his sending terrorists into the US. In 1999, the National Security Council obtained intelligence information --that was not acted on--about Arab individuals who were later identified as participants in the 9/11 attack. Well before the attacks, the CIA tracked two of the 9/11 hijackers to a meeting of known terrorist plotters in Malaysia. There were no watch list entries for these individuals and the CIA was slow to share this information with the FBI. These two hijackers easily entered the US in 2000. Some FBI field agents were doing their job, such as in July 2001 when the Phoenix FBI office told headquarters that Osama bin Laden was sending students to US flight training schools. There are other gaps and failures that contributed to the 9/11 intelligence failure.

Although some progress has been made in intelligence, we are a long way from solving this issue, and it remains a daunting challenge for the DHS.

The third challenge is obtaining and managing funds for homeland security. The FY03 federal budget is currently approved at \$37.7B with state governments at \$10.2B, and local governments at \$19.0B. An estimate of homeland security investments by the private sector was estimated at \$76.5B, but this amount has been subject to study and planning by the private sector. As the US private sector owns and operates 85% of our critical infrastructure, they will have to bear the brunt of the financial burden for homeland security upgrades. Some long term arrangements will have to be made by the DHS with industry for an equitable assessment of who pays how much and for what in protecting our infrastructure from terrorist attacks.

Projected FY04 Homeland Security requested budget is \$36.2 billion, not too different from the FY03 request, but the requirements to adequately fund the 22 newly joined agencies of the DHS, such as the US Coast Guard, Customs, science and technology, etc., under the current budget deficits will not be easy. There are many who feel that the DHS budget is inadequate to take care of the tasks that DHS will be called on to perform—and it will be one of Secretary Ridge's top challenges to ensure that his DHS programs are adequately funded.

The final challenge for the DHS will be meeting the new legal issues of the post 9/11 environment. The Patriot Act, a 342 page document passed soon after the 9/11 attack, has provided our law enforcement agencies with much needed and improved legal powers for dealing with terrorists. Such areas as outdated wiretapping procedures and authorities that were initially based on rotary phone technology need to be updated.

Unfortunately, the Patriot Act and other legal issues, such as the Detention of Terrorist Suspects have been strongly contested by civil rights groups because they allegedly open the door to government abuses that “seriously threaten our democracy.” In particular, librarians and bookstore owners have been reluctant to hand over information about their patron's reading and internet browsing habits—even though there is much evidence that terrorist cells in the US frequently use these resources for their technical research and contacts. These issues along with the authority to share criminal investigative information between intelligence and law enforcement officials are necessary to protect

our national security and are important to the overall success of the DHS counterterrorism operations—but they must have the necessary oversight to avoid potential abuse.

Another Homeland Security legal challenge that needs to be considered is the Total Information Awareness (TIA). The Total Information Awareness project is a DARPA research program in its initial stages to create a quantum leap in the government's ability to access data and databases about private individuals. An intense DARPA research effort to identify suspicious domestic patterns and terrorist threats. It will have the capability to integrate biometric, language processing, and predictive modeling and database technologies (emails, credit purchases, bank accounts and travel plans) to achieve a total information awareness program of potential patterns that will allow us to prevent terrorist attacks. The TIA is essentially aimed at detecting, classifying and identifying foreign terrorists and deciphering their plans

Federal agencies eventually could use TIA-developed technology to share information more effectively and to access information already available to law enforcement and intelligence agencies in a less costly manner. If the research is successful, TIA will provide the intelligence and law enforcement agencies with a powerful and safe tool for unearthing suspected terrorists.

Some in the Congress and civil rights groups have expressed concern over the program, fearing that it might be overly intrusive of American liberty. There are understandable and reasonable worries that giving the government data surveillance capabilities to fight terrorism might lead to unacceptable intrusions into the private lives of law-abiding Americans. Steps are being taken by the TIA office to protect Americans from unwarranted and unnecessary intrusions, such as congressional authorization and strong congressional oversight; absolute protection for fundamental constitutionally protected activity; and equivalency with existing legal restrictions on the government's ability to access data about private individuals.

Technology can be the lynch pin for combating the threat of terrorism. But as we move into highly sophisticated systems like TIA, we will need to ensure that we protect civil liberties while we combat terrorism: