

## Briefing Sheet #1

# Homeland Security: Information Systems Management

---

As we learned from the tragic events of September 11, terrorist attacks can cause major casualties, destruction and disruption across a wide span of jurisdictional boundaries. The outcome and aftermath can overwhelm and overtax the emergency response resources of most localities. To combat such calamities, Information Technology will soon play a critical role in the Defense of the Homeland. Interconnected IT activities will be implemented to head off terrorist attacks within our borders and aid and remedy the areas where terrorist strikes have already occurred.

All levels of government will work together as never seen before. They will strategize and develop effective plans and operations to protect the well being of our citizens. They will need to communicate, coordinate and make decisions quickly to counter any possible terrorist threats. Inter-jurisdictional and inter-agency task forces are now being created to begin the process of defining the Defense of the Homeland operations and assigning responsibilities. As these efforts get under way, Information Technology is being positioned in the forefront to serve in the long-term battle against terrorism.

The following table outlines many of the activities that will be part of the Defense of the Homeland efforts, the agencies that will primarily be tasked with these activities, and some of the IT solution sets that will be used to address them.

Activity	Agencies	Solution Sets
<p><b>Threat Assessment</b>            Evaluating tens of thousands of sensitive sites across the country for the likelihood of potential attacks, assessing the present state of security and proposing new security measures. Also efforts to assess potential cyber terrorist threats.</p>	<ul style="list-style-type: none"> <li>• FBI</li> <li>• FEMA</li> <li>• CDC</li> <li>• State, County &amp; Local Law Enforcement</li> <li>• State &amp; Local Offices of Emergency Services</li> <li>• State &amp; Local Interagency Task Forces, including these agencies:               <ul style="list-style-type: none"> <li>○ Departments of Health</li> <li>○ Departments of Transportation</li> <li>○ Departments of Water Resources</li> <li>○ Departments of Energy</li> <li>○ Fire &amp; Emergency Services</li> <li>○ Departments of Motor Vehicles</li> <li>○ Departments of Parks &amp; Recreation</li> <li>○ Airport, Port, Stadium Authorities</li> <li>○ Departments of Information Technology</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Enhanced Geographic Databases</li> <li>• Relational Databases</li> <li>• Decision Support Systems</li> <li>• Secure Data Networks</li> <li>• Information Assurance</li> <li>• Information Security</li> <li>• Satellite Imaging</li> <li>• Video Conferencing</li> </ul>

Activities	Agencies	Solution Sets
<p><b>Counter Terrorist Activities</b> Intelligence collection, analysis and dissemination to appropriate law enforcement units.</p>	<ul style="list-style-type: none"> <li>• CIA</li> <li>• FBI</li> <li>• State, County &amp; Local Law Enforcement</li> </ul>	<ul style="list-style-type: none"> <li>• Relational Databases</li> <li>• Decision Support Systems</li> <li>• Electronic Intelligence Systems</li> <li>• Secure Data Networks</li> </ul>
<p><b>Threat Reduction</b> New security procedures and systems for airports, buildings, airplanes, roadways, tunnels, ports, waterways, public events, schools and other sensitive sites.</p>	<ul style="list-style-type: none"> <li>• Federal/State Departments of Transportation</li> <li>• Immigration &amp; Naturalization</li> <li>• National Guard</li> <li>• State, County &amp; Local Law Enforcement</li> <li>• State &amp; Local Interagency Task Forces, including these agencies:               <ul style="list-style-type: none"> <li>○ Departments of Health</li> <li>○ Departments of Transportation</li> <li>○ Departments of Water Resources</li> <li>○ Departments of Energy</li> <li>○ Fire &amp; Emergency Services</li> <li>○ Departments of Motor Vehicles</li> <li>○ Departments of Parks &amp; Recreation</li> <li>○ Airport Authorities</li> <li>○ Port Authorities</li> <li>○ Stadium Authorities</li> <li>○ Departments of Information Technology</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Smartcard ID Systems</li> <li>• Facial Recognition Systems</li> <li>• Biometric Security Systems</li> <li>• Security Checkpoint Systems</li> <li>• Relational Databases</li> <li>• Wireless Data and Voice Communications</li> </ul>
<p><b>Threat Response</b> Developing contingency plans, prepositioning disaster relief supplies, training emergency personnel, and coordinating response efforts. Emergency notification to various agencies and volunteers.</p>	<ul style="list-style-type: none"> <li>• FEMA</li> <li>• CDC</li> <li>• National Guard</li> <li>• State &amp; Local Offices of Emergency Services</li> <li>• State, County &amp; Local Law Enforcement</li> </ul>	<ul style="list-style-type: none"> <li>• Enhanced Geographic Databases</li> <li>• Decision Support Systems</li> <li>• Command &amp; Control Centers</li> <li>• Logistical Support Systems</li> <li>• Wireless Data and Voice Communications</li> <li>• Call Centers</li> <li>• Satellite Imaging</li> <li>• Video Teleconferencing</li> </ul>

Activities	Agencies	Solution Sets
<p><b>Disaster Recovery</b>            Establishing command, control and communications at the site of a terrorist incident. Evacuation of wounded and civilians. Providing emergency power, communications and logistical support for rescue effort. Redeployment of critical IT and communications networks in the affected area.</p>	<ul style="list-style-type: none"> <li>• FEMA</li> <li>• National Guard</li> <li>• State, County &amp; Local Law Enforcement</li> <li>• State and Local Offices of Emergency Services</li> </ul>	<ul style="list-style-type: none"> <li>• Mobile Command Centers</li> <li>• Enhanced Geographic Databases</li> <li>• Wireless Voice and Data Communications</li> <li>• Mobile Computing Appliances</li> <li>• Logistical Support Systems</li> <li>• Offsite Data Storage and Backup</li> <li>• Remote Medicine</li> </ul>
<p><b>Information Infrastructure Security</b>            Developing effective countermeasures to cyberterrorism. Protecting critical data and voice networks against physical and cyber attacks.</p>	<ul style="list-style-type: none"> <li>• State &amp; Local Departments of Information Technology</li> <li>• State &amp; Local Law Enforcement</li> </ul>	<ul style="list-style-type: none"> <li>• Firewalls</li> <li>• Virus Protection Software</li> <li>• Cyber Attack Detection Software</li> <li>• Offsite Data Storage &amp; Backup</li> <li>• Disaster Recovery Software</li> <li>• Network Management Software</li> </ul>

Information Technology systems will be used to perform many critical tasks in the Defense of the Homeland efforts and special attention must be given to modernizing critical IT infrastructures in both the public and private sectors. Assessing the risks of cyberterrorism and developing effective countermeasures will be a top priority for state and local governments. Information Technology will be used in both offensive and defensive efforts to identify terrorists and protect our citizens and property.

As we examine the activities involved in the Defense of the Homeland, it is apparent that most of the work will be performed by state and local government agencies. The enhanced geographic databases that will provide the baseline information for threat assessment will have to be developed at the local level. Assessing the current state of security at tens of thousands of sensitive sites across the country will also fall to state and local agency task forces.

The selection of Pennsylvania Gov. Tom Ridge as the new federal director of Homeland Security underscores the central role of state and local government in threat management efforts. Ridge has the responsibility of securing the cooperation of all levels of government in countering the threat of terrorism. Likewise, most states, counties and major municipalities are developing their own interagency task forces to develop Defense of the Homeland programs.

These task force groups are being charged with developing actionable plans within the next 120 to 160 days and deploying Defense of the Homeland solutions within six months to a year. They will be looking for rapidly deployable, commercial off-the-shelf systems (COTS) to meet these new requirements.

Vendors should examine their products and services to see if they can be utilized in Defense of the Homeland efforts. If they have solution sets that can be deployed for these purposes, they should quickly bring them to the attention of the appropriate government customers. Good solutions may be overlooked because vendors fail to explain their applicability.

While other less critical IT deployments may be delayed slightly while new Defense of the Homeland Information Technology systems are being placed on Fast Track deployment schedules, state and local governments are expected to continue their development of e-government systems. Government executives want the efficiencies and cost-savings of e-government so that they can retask resources for other critical areas. The market for non-Defense of the Homeland solutions will still be strong in the state and local government market this year despite the current economic conditions. However, vendors will have to create a clear statement of the value proposition of these systems to help their government customers develop the necessary justifications for these IT projects.

Forecasters say the overall state and local government IT market will surge in 2002 as jurisdictions deploy new systems for e-government as well as for Defense of the Homeland.

For more information on this special Homeland Security Briefing Sheet, contact Rhonda Wilson at 916/932-1321 or [rwilson@centerdigitalgov.com](mailto:rwilson@centerdigitalgov.com).

## ABOUT US

### **Center for Digital Government and Government Technology**

---

The Center for Digital Government is a national research and advisory institute providing government and industry leaders with decision support, research and education services to help them effectively incorporate new technologies in the 21<sup>st</sup> century. *Government Technology* is the nation's leading journal covering Information Technology in state and local government.

The Center for Digital Government and Government Technology are divisions of e.Republic, Inc.,  
100 Blue Ravine Road, Folsom, CA, 95630, 916.932.1300 phone, 916.932.1470 fax.