Information Sharing and Systems

Information contributes to every aspect of homeland security and is a vital foundation for the homeland security effort. Every government official performing every homeland security mission depends upon information and information technology.

Although American information technology is the most advanced in the world, our country's information systems have not adequately supported the homeland security mission. Today, there is no single agency or computer network that integrates all homeland security information nationwide, nor is it likely that there ever will be. Instead, much of the information exists in disparate databases scattered among federal, state, and local entities. In many cases, these computer systems cannot share information—either "horizontally" (across the same level of government) or "vertically" (between federal, state, and local governments). Databases used for law enforcement, immigration, intelligence, and public health surveillance have not been connected in ways that allow us to recognize information gaps or redundancies. As a result, government agencies storing terrorism information, such as terrorist "watch lists," have not been able to systematically share that information with other agencies. These differences can sometimes result in errors if, for example, visa applications and border controls are not checked against consistent "watch lists." It is crucial to link the vast amounts of knowledge resident within each agency at all levels of government.

Despite spending some $50 billion on information technology per year, two fundamental problems have prevented the federal government from building an

efficient government-wide information system. First, government acquisition of information systems has not been routinely coordinated. Over time, hundreds of new systems were acquired to address specific agency requirements. Agencies have not pursued compatibility across the federal government or with state and local entities. Organizations have evolved into islands of technology—distinct networks that obstruct efficient collaboration. Second, legal and cultural barriers often prevent agencies from exchanging and integrating information.

Information-sharing capabilities are similarly deficient at the state and local levels. Many states maintain terrorism, gang, and drug databases that other states cannot access. In addition, there are deficiencies in the communications systems used by municipalities throughout the country. If an attack were to occur today, most state and local first responders would not be using compatible communications equipment. Wireless technology used by most communities is outdated, and one-third of public safety agencies have reported trouble communicating with counterparts during incidents (according to the Public Safety Wireless Network, a joint program of the Departments of Justice and Treasury). Although many states have instituted new infrastructures for sharing information within their jurisdiction, sharing with other states and with federal agencies remains fragmented. This lack of interoperability was evident many times over the past decade—during the 1993 World Trade Center bombing, the 1995 Oklahoma City bombing, the 1999 Columbine school shootings, and the September 11 attacks. At Columbine, the responders included 23 local and county law enforcement agencies, two state and three federal law enforcement agencies, six local fire departments, and seven local emergency medical services—most with incompatible communications procedures and equipment.

National Vision

We will build a national environment that enables the sharing of essential homeland security information. We must build a "system of systems" that can provide the right information to the right people at all times. Information will be shared "horizontally" across each level of government and "vertically" among federal, state, and local governments, private industry, and citizens. With the proper use of people, processes, and technology, homeland security officials throughout the United States can have complete and common awareness of threats and vulnerabilities as well as knowledge of the personnel and resources available to address these threats. Officials will receive the information they need so they can anticipate threats and respond rapidly and effectively. The incorporation of data from all sources across the spectrum of homeland security will assist in border management, critical infrastructure protection, law enforcement, incident management, medical care, and intelligence. In every instance, sensitive and classified information will be scrupulously protected. We will leverage America's leading-edge information technology to develop an information architecture that will effectively secure the homeland.

Major Initiatives

Five principles will guide our country's approach to developing information systems for homeland security. First, we will balance our homeland security requirements with citizens' privacy. Second, the homeland security community will view the federal, state, and local governments as one entity—not from the point of view of any agency or level of government. Third, information will be captured once at the source and used many times to support multiple requirements. Fourth, we will create databases of record, which will be trusted sources of information. Finally, the homeland security information architecture will be a dynamic tool, recognizing that the use of information technology to combat terrorism will continually evolve to stay ahead of the ability of terrorists to exploit our systems.

It is important to protect the public's right to access information, but to do so in balance with security concerns. In general, laws such as the Freedom of Information Act (FOIA) provide for access to government information to the extent that records are not exempt from disclosure. At the same time, Congress has crafted numerous exemptions identifying categories of information that should not be publicly disclosed as the public interest weighs against it. In making decisions about this category of information—such as whether to make it available on agency web sites—agencies must weigh the benefits of certain information to their customers against the risks that freely-available sensitive homeland security information may pose to the interests of the Nation.

Integrate information sharing across the federal government. Under the President's proposal, the Department of Homeland Security will coordinate the sharing of essential homeland security information

nationwide through the Critical Infrastructure Assurance Office. This would include the design and implementation of an interagency information architecture to support efforts to find, track, and respond to terrorist threats in a way that improves both the time of response and the quality of decisions. The Critical Infrastructure Assurance Office will also define pilot projects to address immediate homeland security requirements while laying the foundation for continuous improvement. New coordination groups will recommend better information-sharing methods, focusing on, among other things, border security; transportation security; emergency response; chemical, biological, radiological, and nuclear countermeasures; and infrastructure protection.

As described in the *Domestic Counterterrorism* chapter, the FBI will create a consolidated Terrorism Watch List that includes information from a variety of sources and will be fully accessible to all law enforcement officers and the intelligence community. The Department of Homeland Security, as proposed by the President, will oversee a joint project of the U.S. Customs Service, Immigration and Naturalization Service, Transportation Security Administration, and International Trade Data System Board of Directors for large-scale modernization at border crossings.

Integrate information sharing across state and local governments, private industry, and citizens. Several efforts are underway to enhance the timely dissemination of information from the federal government to state and local homeland security officials by building and sharing law enforcement databases, secure computer networks, secure video teleconferencing capabilities, and more accessible websites.

First, the FBI and other federal agencies are augmenting the information available in their crime and terrorism databases such as the National Crime Information Center and the National Law Enforcement Telecommunications Systems. These databases are accessible to state and local authorities.

Second, state and local governments should use a secure intranet to increase the flow of classified federal information to state and local entities. This would provide a more effective way to disseminate information about changes to the Homeland Security Advisory System and share information about terrorists. The federal government will also make an effort to remove classified information from some documents to facilitate distribution to more state and local authorities. The effort will help state and local law enforcement officials learn when individuals suspected of criminal activity are also under federal investigation and will enable federal officials to link their efforts to investigations being undertaken in the states. The Department of Homeland Security would create a Collaborative Classified Enterprise environment to share sensitive information securely among all relevant government entities. This effort, which is to include dozens of agencies, will put in place a secure communications network to allow agencies to "plug in" their existing databases to share information.

Third, a secure video conferencing capability connecting officials in Washington, D.C. with all government entities in every state will be implemented by the end of the calendar year. This capability will allow federal officials to relay crucial information immediately to state homeland security directors and enhance consultation and coordination.

Fourth, expansion of the '.gov' domain on the Internet for use by state governments has already been completed. In the past, only federal government websites were permitted to use the '.gov' domain. This change will ensure the legitimacy of government websites and enhance searches of all federal and state websites, thereby allowing information to be accessed more quickly. These '.gov' sites will also allow homeland security officials to exchange sensitive information on the secure portions of those websites.

Adopt common "meta-data" standards for electronic information relevant to homeland security. The Administration has begun several initiatives to integrate terrorist-related information from databases of all government agencies responsible for homeland security. As this information is assembled, it is crucial to compile simultaneously information about the information so that homeland security officials understand what is available and where it can be found. This complements the effort to analyze the information with advanced "data-mining" techniques to reveal patterns of criminal behavior and detain suspected terrorists before they act. The Department of Homeland Security, Department of Justice, FBI, and numerous state and local law enforcement agencies would use data-mining tools for the full range of homeland security activities.

The National Spatial Data Infrastructure (NSDI) is a working example of compiling meta-data to facilitate integration of data and support decision making. The NSDI is a network of federal, state, and local geospatial information databases that provide meta-data for all information holdings to make information easier to find and use. The assembled data will include geospatial products, including geographic information systems that will be used with incident management tools and allow immediate display of maps and satellite images. The President's geospatial information integration e-government initiative will increase the amount of meta-data available on the NSDI and

develop data standards that permit additional integration of information. The geospatial e-gov initiative efforts will be coordinated with incident reporting data to create real time maps and images for use across government in domestic counterterrorism and incident management.

Improve public safety emergency communications. In an emergency, rescue personnel cannot afford to be hampered by incompatible communications assets. Under the President's proposal, the Department of Homeland Security will work to develop comprehensive emergency communications systems. The National Communications System would be incorporated into the Department of Homeland Security to facilitate the effort. These systems will disseminate information about vulnerabilities and protective measures, as well as allow first responders to better manage incidents and minimize damage. The new Department would pursue technologies such as "reverse 911" which would call households to alert those at risk. Project SAFECOM, one of the President's e-government initiatives, is being designed to address the Nation's critical public safety wireless shortcomings and will create a tactical wireless infrastructure for first responders and federal, state, and local law enforcement and public safety entities.

Ensure reliable public health information. The Department of Homeland Security, in cooperation with the Department of Health and Human Services, would also work to ensure reliable public health communications. Prompt detection, accurate diagnosis, and timely reporting and investigation of disease epidemics all require reliable communication between medical, veterinary, and public health organizations. Once an attack is confirmed it is crucial to have real-time communication with other hospitals, public health officials, other health professionals, law enforcement, emergency management officials, and the media. The Centers for Disease Control and Prevention has created the Health Alert Network to increase the interconnectivity of federal, state, and local public health and emergency response agencies for timely communications about health advisories, laboratory findings, information about disease outbreaks, and distance learning. Under this plan, 90 percent of every state will be covered by this high-speed network and the capacity to receive emergency broadcast health alert messages. Providing the public timely and accurate risk communication during a public health emergency will inform as well as reassure concerned Americans.