

Using 21st Century Technology to Defend the Homeland

America's information infrastructure is a source of both great strength and considerable vulnerability. The President recognizes that modern information technology is essential not only for making our Nation more prosperous but for making our homeland more secure. The President has launched a long-term program for using advanced information management technology to better protect the Nation. At the same time, the President's 2003 Budget requests significant funding for cyberspace security, an essential new mission for the 21st century given our growing dependence on critical information infrastructure, most importantly the Internet.

Information Technology and the Federal Government: Expanding E-Government

The Budget for 2003 requests a total of \$50 billion for information technology investment across the entire Federal government. This enormous Federal investment in technology represents an opportunity to improve the performance of billions of dollars of Federal spending by increasing the effectiveness and efficiency of government.

Led by the Office of Management and Budget, the Administration is deploying 21 high payoff e-government initiatives to maximize Federal government productivity gains from technology, eliminate redundant systems, and significantly improve government's quality of service for citizens, businesses, and other levels of government over the next 18 to 24 months.

Using Information to Secure the Homeland

The President believes that an effective use of intelligence and closer coordination across all levels of government will help stop future terrorist attacks. In the wake of September 11, for example, we discovered that information on the hijackers' activities was available through a variety of databases at the Federal, State, and local government levels as well as within the private sector. Looking forward, we must build a system that combines threat information and then transmits it as needed to all relevant law enforcement and public safety officials.

The President's budget calls for an increase of \$722 million and sets in motion a program to use information technology to more effectively share information and intelligence, both horizontally (among Federal agencies and Departments) and vertically (among the Federal, State and local governments). This ongoing homeland security initiative is a key component of the President's "Expanded Electronic Government" management initiative for the entire Federal government, which seeks to improve the way that agencies work together to serve citizens by maximizing the benefits of the Federal government's overall investment in information technology.

The homeland security information initiative has two key objectives:

- **Goal 1: Tear down unwarranted information "stovepipes" within the Federal government.** The President's Budget for 2003 proposes to establish an Information Integration Office within the Department of Commerce to implement a number of priority homeland security goals in the area of horizontal information sharing. The most important function of this office will be to design and help implement an interagency information architecture that will support United States efforts to find, track, and respond to terrorist threats within the United States and around the world, in a way that improves both the time of response and the quality of decisions. Controls

will be developed to ensure that this initiative is carried out in a manner consistent with our broader values of civil liberties, economic prosperity, and privacy.

Information technology is also a key to keeping track of short-term foreign visitors. Currently, the country has no system in place for monitoring when a foreign visitor has overstayed his or her visa. To begin filling this gap, the President's 2003 Budget provides \$380 million to the INS to implement a new entry-exit system to track the arrival and departure of non-U.S. citizens. This new information-based system will dramatically improve our ability to deny access to those individuals who should not enter the United States, while speeding the entry of routine, legitimate traffic.

- **Goal 2: Share homeland security information with States, localities, and relevant private sector entities.** The struggle against terrorism is a truly national struggle. Federal, State, and local government agencies, as well as the private sector, must work seamlessly together. Having the right system of communication - content, process, and infrastructure - is critical to bridging the existing gaps between the Federal, State, and local governments, as well as the private sector. These new systems will greatly assist our officials at all levels to protect and defend against future terrorist attacks, and to effectively manage incidents whenever they should occur.

To help meet these needs, the Administration will establish a uniform national threat advisory system to inform Federal agencies, State and local officials, as well as the private sector, of terrorist threats and appropriate protective actions. The Budget for 2003 supports this effort by funding the development and implementation of secure information systems to streamline the dissemination of critical homeland security information.

Cyberspace-Security: Protecting our Information Infrastructure

The information technology revolution has changed the way business is transacted, government operates and national defence is conducted.

These three functions are now fueled by an interdependent network of critical information infrastructures of which the Internet is key. America must do more to strengthen security on the Internet to protect our critical infrastructure. This cannot be done through government regulation; it can only be accomplished through a voluntary public and private partnership, including corporate and non-governmental organizations.

The President recognized the importance of ensuring the continued operation of America's critical information services by creating a national board and designating a special advisor for cyberspace security. Since October 2001, the President's Critical Infrastructure Protection Board has organized national committees to streamline initiatives and address emergency planning. The board has initiated research into potential methods to isolate and protect critical government information that carries vital communications. It has fostered an unprecedented national government-industry partnership to provide alert and warning for cyberspace threats. This comprehensive strategy to defend cyberspace will be the result of a true partnership among government and the owners and operatives of critical infrastructure - including our partnership with the information technology industry, telecommunications, electric power, and the financial services industries. Some of the components of this national strategy will include:

National Infrastructure Protection Center (NIPC).

The President's Budget for 2003 requests \$125 million to fund the NIPC, the premier cyberspace-threat response center located within the FBI. This request represents an increase of more than \$50 million from the NIPC's base 2002 funding level.

Cyberspace Warning Intelligence Network.

The Internet and our critical infrastructure are constantly under attack from viruses and other invasive programs. The President's Budget for 2003 requests \$30 million to create the Cyberspace Warning Intelligence Network (CWIN) that would link the major players in government and the private sector to manage future cyberspace crises.

Priority Wireless Access.

On September 11, we learned first hand that in times of a major crisis, wireless communication jams due to congestion. First responders must be able to complete calls in a timely manner. The President's Budget for 2003 requests \$60 million to develop a wireless priority access program that will give authorized users priority on the cellular network. The program will ensure that first responders have priority for cellular phone coverage during emergencies.

National Infrastructure Simulation and Analysis Center.

The President's Budget for 2003 requests \$20 million to fund the National Infrastructure Simulation and Analysis Center at the Department of Energy. This Center will promote collaboration between Federal research efforts and the private sector to better understand the dependencies between the Internet, our critical infrastructure, and our economy.

Secure "GovNet" Feasibility Study.

The President's Budget for 2003 requests \$5 million for a feasibility study of a proposal to develop a government network that will secure critical functions performed by government at a higher level of security against external attack.

Advanced Encryption Standard.

The President helped foster better computer security at Federal agencies. A new Federal standard announced on December 4, 2001, is designed to protect sensitive, unclassified information well into the 21st century. In limited circumstances, it will also be available for classified national security information. The new standard, called the Advanced Encryption Standard, also is expected to be used widely in the private sector, benefiting millions of consumers and businesses.

Cybercorps Scholarships for Service.

The President's Budget for 2003 requests \$11 million for the "Cybercorps." By injecting scholarship funding into universities across America, the Cybercorps Scholarship for Service program encourages college students to become high tech computer security professionals within government. Managed by the National Science Foundation and the Office of Personnel Management, this program also helps to build academic programs at universities in the area of computer security.