

- All applications for U.S. visas are checked against extensive databases with terrorism-related information and all international air and sea passengers are vetted against our consolidated terrorist watchlist.
- As of October 2005, all Visa Waiver Program countries are required to have biometric passports.
- The Transportation Security Administration (TSA) screens 100 percent of commercial air passengers and bags.
- TSA is directing Registered Traveler program providers to collect ten fingerprint images from each applicant and to store biometric data for identity confirmations using smart card technology that conforms to current Federal Technical Implementation Guidance.
- The United States Government also is unveiling new comprehensive screening and credentialing initiatives, such as the Real ID Act and Western Hemisphere Travel Initiative, improving access to lost and stolen travel document information, and the e-passport to strengthen our ability to identify those crossing our borders.
- In March 2005, the U.S., Mexico, and Canada launched the Security and Prosperity Partnership of North America (SPP). Through this initiative, we are making measurable progress on a number of security issues affecting our three countries and have strengthened relationships in the areas of preparedness, law enforcement, and the screening of travelers and cargo.

Critical Infrastructure Protection

- DHS has released the National Infrastructure Protection Plan, which provides a comprehensive risk management framework that clearly defines critical infrastructure protection roles and responsibilities for all levels of government, private industry, nongovernmental agencies, and tribal partners.
- DHS has implemented the Buffer Zone Protection Program, which provides grant funding to protect and secure areas surrounding critical infrastructure and key resource sites such as chemical facilities, dams, and nuclear plants across the country. DHS worked in conjunction with local law enforcement authorities throughout the Nation to submit more than 1400 plans on grant allocations for enhanced security around critical infrastructure.
- DHS has established the Homeland Infrastructure Threat and Risk Assessment Center (HITRAC), where intelligence analysts and infrastructure specialists work to identify the threat to critical infrastructures, vulnerabilities and interdependencies, and the overall risk inherent in any potential attack against critical infrastructure. The HITRAC works closely with critical infrastructure owners and operators to ensure that the most complete, actionable, accurate information regarding private sector assets is disseminated expeditiously to key stakeholders. The HITRAC also provides recommended protective measures.
- The United States also has established the National Cyber Response Coordination Group (NCRCG) as the Federal Government's principal interagency mechanism to coordinate efforts to respond to and recover from cyber incidents of national significance.