(k) recommended research and development on technologies designed to enhance screening effectiveness and further protect privacy interests; and

(l) a plan for incorporating known traveler programs into the screening procedures, where appropriate.

(7) Not later than 90 days after the date of this directive, the Secretary of Homeland Security, in coordination with the heads of the Federal departments and agencies listed in section 4 of this directive, shall also provide to me, through the Assistant to the President for Homeland Security and the Director of the Office of Management and Budget, a prioritized investment and implementation plan for a systematic approach to terrorist-related screening that optimizes detection and interdiction of suspected terrorists and terrorist activities. The plan shall describe the scope, governance, principles, outcomes, milestones, training objectives, metrics, costs, and schedule of activities to implement the policy set forth in section 1 of this directive. The Secretary of Homeland Security shall further provide a report on the status of the implementation of the plan to me through the Assistant to the President for Homeland Security 6 months after the date of this directive and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

(8) In order to ensure comprehensive and coordinated terrorist-related screening procedures, the implementation of this directive shall be consistent with Government-wide efforts to improve information sharing. Additionally, the reports and plan required under sections 4 and 7 of this directive shall inform development of Government-wide information sharing improvements.

(9) This directive does not alter existing authorities or responsibilities of department and agency heads including to carry out operational activities or provide or receive information. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees, or agents, or any other person.

GEORGE W. BUSH

Homeland Security Presidential Directive/HSPD–12—Policy for a Common Identification Standard for Federal Employees and Contractors

August 27, 2004

Subject: Policy for a Common Identification Standard for Federal Employees and Contractors

(1) Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

(2) To implement the policy set forth in paragraph (1), the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the "Standard") not later than 6 months

after the date of this directive in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The Secretary of Commerce shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.

(3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).

(4) Not later than 4 months following promulgation of the Standard, the heads of executive departments and agencies shall have a program in place to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the Standard. As promptly as possible, but in no case later than 8 months after the date of promulgation of the Standard, the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. Departments and agencies shall implement this directive in a manner consistent with ongoing Government-wide activities, policies and guidance issued by OMB, which shall ensure compliance.

(5) Not later than 6 months following promulgation of the Standard, the heads of executive departments and agencies shall identify to the Assistant to the President for Homeland Security and the Director of OMB those Federally controlled facilities, Federally controlled information systems, and other Federal applications that are important for security and for which use of the Standard in circumstances not covered by this directive should be considered. Not later than 7 months following the promulgation of the Standard, the Assistant to the President for Homeland Security and the Director of OMB shall make recommendations to the President concerning possible use of the Standard for such additional Federal applications.

(6) This directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans.

(7) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.

(8) The Assistant to the President for Homeland Security shall report to me not later than 7 months after the promulgation of the Standard on progress made to implement this directive, and shall thereafter report to me on such progress or any

recommended changes from time to time as appropriate.

GEORGE W. BUSH

The President's Radio Address
August 28, 2004

Good morning. In the 3 years since our country was attacked, America has remained on the offensive against terrorist enemies wherever they hide and plot. Part of that offensive has been to reorganize our Government so that all our intelligence and law enforcement agencies cooperate effectively to expose and disrupt threats against America.

The Commission on Terrorist Attacks Upon the United States, also known as the 9/11 Commission, concluded that these efforts have made America safer. They also concluded that America is still not safe. I agree with both of those conclusions, and so my administration is taking additional actions to reform our intelligence services and improve America's ability to find, track, and stop dangerous terrorists.

This week, I signed a series of Executive orders to ensure that the people in Government responsible for defending America and countering terrorism have the best possible information and support to identify threats and to protect the homeland. Some of these orders reflect specific recommendations of the 9/11 Commission. All of them are essential to America's security as we wage the war on terror.

First, I have ordered the Director of Central Intelligence to perform the functions of the National Intelligence Director within the constraints of existing law, until Congress establishes that position. I agree with the 9/11 Commission that America needs a single official to coordinate the foreign and domestic activities of the intelligence community with authority over personnel, budgeting, and policy. I am working with Members of Congress to create this position, and while we act, the Director of Central Intelligence will play an expanded role. I also urge Congress to act swiftly on my nomination of Porter Goss, a proven reformer with decades of experience in intelligence to lead the CIA.

Second, I have ordered the establishment of a National Counterterrorism Center. This new center builds on the capabilities of the Terrorist Threat Integration Center, which I created more than a year ago. The Center will become our Government's central knowledge bank for information about known and suspected terrorists and will help ensure effective joint action across the Government so that our efforts against terrorists are unified in priority and purpose. Center personnel will also prepare the daily terrorism threat report that comes to me and to senior Government officials.

Third, we're making sure that all agencies of our Government share vital threat information. I have ordered the Director of Central Intelligence to ensure that we have common standards and clear accountability measures for intelligence sharing across the agencies of our Government. I have established a new Information Systems Council to identify and break down any remaining barriers to the rapid sharing of threat information by America's intelligence agencies, law enforcement agencies, and State and local governments. To continue to protect the freedoms and privacy of our citizens, I've established a Civil Liberties Board to monitor information-sharing practices.