AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Executive Order 13356—Strengthening the Sharing of Terrorism Information To Protect Americans

August 27, 2004

By the authority vested in me as President by the Constitution and laws of the United States of America, and in order to further strengthen the effective conduct of United States intelligence activities and protect the territory, people, and interests of the United States of America, including against terrorist attacks, it is hereby ordered as follows:

Section 1. *Policy.* To the maximum extent consistent with applicable law, agencies shall, in the design and use of information systems and in the dissemination of information among agencies:

(a) give the highest priority to (i) the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America, (ii) the interchange of terrorism information among agencies, (iii) the interchange of terrorism information between agencies and appropriate authorities of States and local governments, and (iv) the protection of the ability of agencies to acquire additional such information; and

(b) protect the freedom, information privacy, and other legal rights of Americans in the conduct of activities implementing subsection (a).

Sec. 2. *Duty of Heads of Agencies Possessing or Acquiring Terrorism Information.* To implement the policy set forth in section 1 of this order, the head of each agency that possesses or acquires terrorism information:

(a) shall promptly give access to the terrorism information to the head of each other agency that has counterterrorism functions, and provide the terrorism information to each such agency in accordance with the standards and information sharing guidance issued pursuant to this order, unless otherwise directed by the President, and consistent with (i) the statutory responsibilities of the agencies providing and receiving the information, (ii) any guidance issued by the Attorney General to fulfill the policy set forth in subsection 1(b) of this order, and (iii) other applicable law, including section 103(c)(7) of the National Security Act of 1947, section 892 of the Homeland Security Act of 2002, Executive Order 12958 of April 17, 1995, as amended, and Executive Order 13311 of July 29, 2003;

(b) shall cooperate in and facilitate production of reports based on terrorism information with contents and formats that permit dissemination that maximizes the utility of the information in protecting the territory, people, and interests of the United States; and

(c) shall facilitate implementation of the plan developed by the Information Systems Council established by section 5 of this order.

Sec. 3. *Preparing Terrorism Information for Maximum Distribution within Intelligence Community.* To assist in expeditious and effective implementation by agencies within the Intelligence Community of the policy set forth in section 1 of this order, the Director of Central Intelligence shall, in consultation with the Attorney General and the other heads of agencies within the Intelligence Community, set forth not later than 90 days after the date of this order, and thereafter as appropriate, common standards for the sharing of terrorism information by agencies within the Intelligence Community with (i) other agencies within the Intelligence Community, (ii) other agencies having counterterrorism functions, and (iii) through or in coordination with the Department of Homeland Security, appropriate authorities of State and local governments. These common standards shall improve information sharing by such methods as:

(a) requiring, at the outset of the intelligence collection and analysis process, the creation of records and reporting, for both raw and processed information including, for example, metadata and content, in such a manner that sources and methods are protected so that the information can be distributed at lower classification levels, and by creating unclassified versions for distribution whenever possible;

(b) requiring records and reports related to terrorism information to be produced with multiple versions at an unclassified level and at varying levels of classification, for example

on an electronic tearline basis, allowing varying degrees of access by other agencies and personnel commensurate with their particular security clearance levels and special access approvals;

(c) requiring terrorism information to be shared free of originator controls, including, for example, controls requiring the consent of the originating agency prior to the dissemination of the information outside any other agency to which it has been made available, to the maximum extent permitted by applicable law, Executive Orders, or Presidential guidance;

(d) minimizing the applicability of information compartmentalization systems to terrorism information, to the maximum extent permitted by applicable law, Executive Orders, and Presidential guidance; and

(e) ensuring the establishment of appropriate arrangements providing incentives for, and holding personnel accountable for, increased sharing of terrorism information, consistent with requirements of the Nation's security and with applicable law, Executive Orders, and Presidential guidance.

Sec. 4. *Requirements for Collection of Terrorism Information Inside the United States.* (a) The Attorney General, the Secretary of Homeland Security, and the Director of Central Intelligence shall, not later than 90 days after the date of this order, jointly submit to the President, through the Assistants to the President for National Security Affairs and Homeland Security, their recommendation on the establishment of executive branch-wide collection and sharing requirements, procedures, and guidelines for terrorism information to be collected within the United States, including, but not limited to, from publicly available sources, including nongovernmental databases.

(b) The recommendation submitted under subsection (a) of this section shall also:

(i) address requirements and guidelines for the collection and sharing of other information necessary to protect the territory, people, and interests of the United States; and

(ii) propose arrangements for ensuring that officers of the United States with responsibilities for protecting the territory, people, and interests of the United States are provided with clear, understandable, consistent, effective, and lawful procedures and guidelines for the collection, handling, distribution, and retention of information.

Sec. 5. *Establishment of Information Systems Council.* (a) There is established an Information Systems Council (Council), chaired by a designee of the Director of the Office of Management and Budget, and composed exclusively of designees of: the Secretaries of State, the Treasury, Defense, Commerce, Energy, and Homeland Security; the Attorney General; the Director of Central Intelligence; the Director of the Federal Bureau of Investigation; the Director of the National Counterterrorism Center, once that position is created and filled (and until that time the Director of the Terrorism Threat Integration Center); and such other heads of departments or agencies as the Director of the Office of Management and Budget may designate.

(b) The mission of the Council is to plan for and oversee the establishment of an interoperable terrorism information sharing environment to facilitate automated sharing of terrorism information among appropriate agencies to implement the policy set forth in section 1 of this order.

(c) Not later than 120 days after the date of this order, the Council shall report to the President through the Assistants to the President for National Security Affairs and Homeland Security, on a plan, with proposed milestones, timetables for achieving those milestones, and identification of resources, for the establishment of the proposed interoperable terrorism information sharing environment. The plan shall, at a minimum:

(i) describe and define the parameters of the proposed interoperable terrorism information sharing environment, including functions, capabilities, and resources;

(ii) identify and, as appropriate, recommend the consolidation and elimination of current programs, systems, and processes used by agencies to share terrorism information, and recommend as appropriate the redirection of existing resources to support

the interoperable terrorism information sharing environment;

(iii) identify gaps, if any, between existing technologies, programs, and systems used by agencies to share terrorism information and the parameters of the proposed interoperable terrorism information sharing environment;

(iv) recommend near-term solutions to address any such gaps until the interoperable terrorism information sharing environment can be established;

(v) recommend a plan for implementation of the interoperable terrorism information sharing environment, including roles and responsibilities, measures of success, and deadlines for the development and implementation of functions and capabilities from the initial stage to full operational capability;

(vi) recommend how the proposed interoperable terrorism information sharing environment can be extended to allow interchange of terrorism information between agencies and appropriate authorities of States and local governments; and

(vii) recommend whether and how the interoperable terrorism information sharing environment should be expanded, or designed so as to allow future expansion, for purposes of encompassing other categories of intelligence and information.

Sec. 6. *Definitions.* As used in this order:

(a) the term "agency" has the meaning set forth for the term "executive agency" in section 105 of title 5, United States Code, together with the Department of Homeland Security, but includes the Postal Rate Commission and the United States Postal Service and excludes the Government Accountability Office;

(b) the terms "Intelligence Community" and "agency within the Intelligence Community" have the meanings set forth for those terms in section 3.4(f) of Executive Order 12333 of December 4, 1981, as amended;

(c) the terms "local government," "State," and, when used in a geographical sense, "United States," have the meanings set forth for those terms in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101); and

(d) the term "terrorism information" means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other United States Government activities, relating to (i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; (iii) communications of or by such groups or individuals; or (iv) information relating to groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Sec. 7. *General Provisions.* (a) This order:

(i) shall be implemented in a manner consistent with applicable law, including Federal law protecting the information privacy and other legal rights of Americans, and subject to the availability of appropriations;

(ii) shall be implemented in a manner consistent with the authority of the principal officers of agencies as heads of their respective agencies, including under section 199 of the Revised Statutes (22 U.S.C. 2651), section 201 of the Department of Energy Reorganization Act (42 U.S.C. 7131), section 102(a) of the National Security Act of 1947 (50 U.S.C. 403(a)), section 102(a) of the Homeland Security Act of 2002 (6 U.S.C. 112(a)), and sections 301 of title 5, 113(b) and 162(b) of title 10, 1501 of title 15, 503 of title 28, and 301(b) of title 31, United States Code; and

(iii) shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals.

(b) This order is intended only to improve the internal management of the Federal Government and is not intended to, and does

not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, instrumentalities, or entities, its officers, employees, or agents, or any other person.

George W. Bush

The White House,
August 27, 2004.

[Filed with the Office of the Federal Register, 8:45 a.m., August 31, 2004]

NOTE: This Executive order will be published in the *Federal Register* on September 1.

Directive on Comprehensive Terrorist-Related Screening Procedures

August 27, 2004

Homeland Security Presidential Directive/ HSPD–11

Subject: Comprehensive Terrorist-Related Screening Procedures

(1) In order more effectively to detect and interdict individuals known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism ("suspected terrorists") and terrorist activities, it is the policy of the United States to:

(a) enhance terrorist-related screening (as defined below) through comprehensive, coordinated procedures that detect, identify, track, and interdict people, cargo, conveyances, and other entities and objects that pose a threat to homeland security, and to do so in a manner that safeguards legal rights, including freedoms, civil liberties, and information privacy guaranteed by Federal law, and builds upon existing risk assessment capabilities while facilitating the efficient movement of people, cargo, conveyances, and other potentially affected activities in commerce; and

(b) implement a coordinated and comprehensive approach to terrorist-related screening—in immigration, law enforcement, intelligence, counterintelligence, and protection of the border, transportation systems, and critical infrastructure—that supports homeland security, at home and abroad.

(2) This directive builds upon HSPD–6, "Integration and Use of Screening Information to Protect Against Terrorism." The Terrorist Screening Center (TSC), which was established and is administered by the Attorney General pursuant to HSPD–6, enables Government officials to check individuals against a consolidated Terrorist Screening Center Database. Other screening activities underway within the Terrorist Threat Integration Center (TTIC) and the Department of Homeland Security further strengthen the ability of the United States Government to protect the people, property, and territory of the United States against acts of terrorism.

(3) In this directive, the term "terrorist-related screening" means the collection, analysis, dissemination, and use of information related to people, cargo, conveyances, and other entities and objects that pose a threat to homeland security. Terrorist-related screening also includes risk assessment, inspection, and credentialing.

(4) Not later than 75 days after the date of this directive, the Secretary of Homeland Security, in coordination with the Attorney General, the Secretaries of State, Defense, Transportation, Energy, Health and Human Services, Commerce, and Agriculture, the Directors of Central Intelligence and the Office of Management and Budget, and the heads of other appropriate Federal departments and agencies, shall submit to me, through the Assistant to the President for Homeland Security, a report setting forth plans and progress in the implementation of this directive, including as further described in sections 5 and 6 of this directive.

(5) The report shall outline a strategy to enhance the effectiveness of terrorist-related screening activities, in accordance with the policy set forth in section 1 of this directive, by developing comprehensive, coordinated, systematic terrorist-related screening procedures and capabilities that also take into account the need to: