

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

that is descriptive and specific to an event or activity, and is more than a label. For example, “Subject X provides false travel documentation for Al-Qaida operatives” is PARTICULARIZED DEROGATORY INFORMATION, whereas “Subject Y is a supporter,” standing alone, is not considered PARTICULARIZED DEROGATORY INFORMATION.

- R. **POSITIVE MATCH:** occurs when the TSC determines that information about a subject encountered by a SCREENER exactly or reasonably matches a record in the TSDB.
- S. **POTENTIAL MATCH:** occurs when an ENCOUNTERING AGENCY believes it has a match with a KNOWN or SUSPECTED TERRORIST record in the TSDB. An ENCOUNTERING AGENCY may attempt to resolve POTENTIAL MATCHES first through its review process. If an ENCOUNTERING AGENCY’S review process cannot resolve the individual’s status as not a match to a TSDB record, the ENCOUNTERING AGENCY will refer the POTENTIAL MATCH to TSC for final adjudication.
- T. **PURELY DOMESTIC TERRORISM INFORMATION:** is defined in the *TSC MOU* as information about U.S. PERSONS that has been determined to be PURELY DOMESTIC TERRORISM INFORMATION with “no link to foreign intelligence, counterintelligence, or international TERRORISM.”
- U. **REASONABLE SUSPICION:** is the standard that must be met in order to include an individual in the TSDB, absent an exception provided for in the Watchlisting Guidance. To meet the REASONABLE SUSPICION standard, the NOMINATOR, based on the totality of the circumstances, must rely upon articulable intelligence or information which, taken together with rational inferences from those facts, reasonably warrants a determination that an individual is known or suspected to be or has been knowingly engaged in conduct constituting, in preparation for, in aid of, or related to TERRORISM and/or TERRORIST ACTIVITIES. There must be an objective factual basis for the NOMINATOR to believe that the individual is a KNOWN or SUSPECTED TERRORIST. Mere guesses or hunches are not enough to constitute a REASONABLE SUSPICION that an individual is a KNOWN or SUSPECTED TERRORIST. Reporting of suspicious activity alone that does not meet the REASONABLE SUSPICION standard set forth herein is not a sufficient basis to watchlist an individual. The facts, however, given fair consideration, should sensibly lead to the conclusion that an individual is, or has, engaged in TERRORISM and/or TERRORIST ACTIVITIES.
- V. **SCREENER:** a Department or Agency that is authorized to conduct TERRORISM screening to determine if an individual is a possible match to a KNOWN or SUSPECTED TERRORIST in the TSDB. SCREENERS can include Federal Departments or Agencies, state, local, tribal, territorial, or foreign governments and certain private entities. The term ‘SCREENER’ is used throughout this document as a general reference to a government official who compares an individual’s information with information in the TSDB to determine if an individual is in the TSDB. Law enforcement officials who engage in such activities may normally describe their targeting or other actions in this context as other than “screening.” For ease of reference, government officials who compare an individual’s information with information in the TSDB will be referred to in the Watchlisting Guidance as a “SCREENER.”
- W. **SUSPECTED TERRORIST:** is an individual who is REASONABLY SUSPECTED to be, or has been engaged in conduct constituting, in preparation for, in aid of, or related to TERRORISM and/or TERRORIST ACTIVITIES based on an articulable and REASONABLE SUSPICION.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

Appendix I

- X. TARGETED ANALYSIS:** is further exploitation of a targeted set of ENCOUNTER PACKAGES and ADVANCED ANALYSIS products to assist in identifying TERRORIST trends and changes to methods, tactics, and practices. ENCOUNTERS for TARGETED ANALYSIS are selected using contemporaneous threat criteria, and research in additional repositories. Contemporaneous threat criteria include association with a priority terrorist group (e.g., NIPF Tier I or II); ENCOUNTERS with KNOWN or SUSPECTED TERRORISTS designated as No Fly or associated with violent activity; or at the request of any Department or Agency that identifies a need.
- Y. TERRORISM AND/OR TERRORIST ACTIVITIES:** is a combination of definitions because none of the federal law definitions of “terrorism” or “terrorist activities” were directly applicable to the consolidated approach to watchlisting. For terrorist watchlisting purposes under this Watchlisting Guidance, “terrorism and/or terrorist activities” combine elements from various federal definitions and are considered to: (a) involve violent acts or acts dangerous to human life, property, or infrastructure that may be a violation of U.S. law, or may have been, if those acts were committed in the United States; and, (b) appear intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of government by mass destruction, assassination, kidnapping, or hostage-taking. This includes activities that facilitate or support TERRORISM and/or TERRORIST ACTIVITIES, such as providing a safe house, transportation, communications, funds, transfer of funds or other material benefit, false documentation or identification, weapons (including chemical, biological, or radiological weapons), explosives, or training for the commission of act of terrorism and/or TERRORIST ACTIVITY.
- Z. TERRORISM INFORMATION:** applies, where appropriate, to purely domestic terrorism as defined in the TSC MOU and incorporates the definition found in in section 1016 of the IRTPA (6 U.S.C. 485), as amended. The term “TERRORISM INFORMATION” means –
1. all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—
    - a) 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;
    - b) threats posed by such groups or individuals to the United States, U.S. PERSONS, or United States interests, or to those of other nations;
    - c) communications of or by such groups or individuals; or
    - d) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and
  2. includes weapons of mass destruction information.
    - a) **Weapons of Mass Destruction Information:** information that could reasonably be expected to assist in the development, proliferation, or use of a weapon of mass destruction (including a chemical, biological,

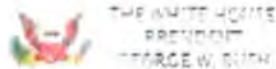
UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

radiological, or nuclear weapon) that could be used by a TERRORIST or a terrorist organization against the United States, including information about the location of any stockpile of nuclear materials that could be exploited for use in such a weapon that could be used by a TERRORIST or a terrorist organization against the United States.

- AA. TERRORISM SCREENING INFORMATION:** is defined in the standard HSPD-6 agreement to mean unclassified identifying information about KNOWN or SUSPECTED TERRORISTS.
- BB. TERRORIST:** please see KNOWN TERRORIST or SUSPECTED TERRORIST.
- CC. TERRORIST IDENTIFIERS:** are referred to in the *TSC MOU* as U//FOUO data for inclusion into the TSDB. TERRORIST IDENTIFIERS are data points about a particular identity that include names and aliases, dates of birth, places of birth, unique identifying numbers, passport information, country of origin and nationality, physical identifiers, addresses, photographs or renderings of the individual, fingerprints or other biometric data, employment data, license plate numbers, and any other TERRORISM INFORMATION that ORIGINATORS specifically provide for passage to the TSC.
- DD. TERRORIST INFORMATION:** as defined in HSPD-6 is “information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to TERRORISM.”
- EE. U.S. PERSON:** is defined in Executive Order 12333 (as amended) as “a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.” The Watchlisting Guidance contains certain exceptions to the minimum substantive derogatory standards for TERRORIST watchlisting that support immigration and visa screening activities by the DHS and DOS to determine whether ineligibilities exist for admission to the United States or visa adjudication pursuant to the INA. Because the INA defines “aliens” as any person not a citizen or national of the United States, the INA admissibility provisions also apply to LPRs, in certain circumstances, who are considered as U.S. PERSONS under Executive Order 12333. Consequently, NCTC developed a mechanism in TIDE to identify and distinguish U.S. citizens from non-U.S. citizens in order to further distinguish between “aliens” under the INA and U.S. PERSONS under Executive Order 12333. See INA § 101(a)(3) [8 U.S.C. 1101(a)(3)].

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**



For Immediate Release  
Office of the Press Secretary  
September 16, 2003

Appendix 2

## Homeland Security Presidential Directive/Hspd-6

Subject: Integration and Use of Screening Information

To protect against terrorism it is the policy of the United States to (1) develop, integrate, and maintain thorough, accurate, and current information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (Terrorist Information); and (2) use that information as appropriate and to the full extent permitted by law to support (a) Federal, State, local, territorial, tribal, foreign-government, and private-sector screening processes, and (b) diplomatic, military, intelligence, law enforcement, immigration, visa, and protective processes.

This directive shall be implemented in a manner consistent with the provisions of the Constitution and applicable laws, including those protecting the rights of all Americans.

To further strengthen the ability of the United States Government to protect the people, property, and territory of the United States against acts of terrorism, and to the full extent permitted by law and consistent with the policy set forth above:

- (1) The Attorney General shall establish an organization to consolidate the Government's approach to terrorism screening and provide for the appropriate and lawful use of Terrorist Information in screening processes.
- (2) The heads of executive departments and agencies shall, to the extent permitted by law, provide to the Terrorist Threat Integration Center (TTIC) on an ongoing basis all appropriate Terrorist Information in their possession, custody, or control. The Attorney General, in coordination with the Secretary of State, the Secretary of Homeland Security, and the Director of Central Intelligence shall implement appropriate procedures and safeguards with respect to all such information about United States persons. The TTIC will provide the organization referenced in paragraph (1) with access to all appropriate information or intelligence in the TTIC's custody, possession, or control that the organization requires to perform its functions.
- (3) The heads of executive departments and agencies shall conduct screening using such information at all appropriate opportunities, and shall report to the Attorney General not later than 90 days from the date of this directive, as to the opportunities at which such screening shall and shall not be conducted.
- (4) The Secretary of Homeland Security shall develop guidelines to govern the use of such information to support State, local, territorial, and tribal screening processes, and private sector screening processes that have a substantial bearing on homeland security.
- (5) The Secretary of State shall develop a proposal for my approval for enhancing cooperation with certain foreign governments, beginning with those countries for which the United States has waived visa requirements, to establish appropriate access to terrorism screening information of the participating governments.

This directive does not alter existing authorities or responsibilities of department and agency heads to carry out operational activities or provide or receive information. This directive is intended only to improve the internal management of the executive branch and 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.

The Attorney General, in consultation with the Secretary of State, the Secretary of Homeland Security, and the Director of Central Intelligence, shall report to me through the Assistant to the President for Homeland Security not later than October 31, 2003, 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 SECRETARY OF STATE  
THE ATTORNEY GENERAL  
THE SECRETARY OF HOMELAND SECURITY  
THE DIRECTOR OF CENTRAL INTELLIGENCE

MEMORANDUM OF UNDERSTANDING  
ON THE INTEGRATION AND USE OF SCREENING INFORMATION  
TO PROTECT AGAINST TERRORISM

(1) This memorandum represents the consensus view of the Secretary of State, the Attorney General, the Secretary of Homeland Security, and the Director of Central Intelligence regarding the implementation of Homeland Security Presidential Directive-6 (HSPD-6), dated September 16, 2003, entitled "Integration and Use of Screening Information to Protect Against Terrorism." (U)

(2) Consistent with the President's direction, the Parties to this Memorandum will develop and maintain, to the extent permitted by law, the most thorough, accurate, and current information possible about individuals known or appropriately suspected to be or have been involved in activities constituting, in preparation for, in aid of, or related to terrorism ("Terrorist Information"), and will, as described in this Memorandum:

(a) use that information to support screening processes at all appropriate opportunities;

(b) make accessible appropriate information to State, local, territorial, and tribal authorities to support their screening processes and otherwise enable them to identify, or assist in identifying, such individuals;

(c) host mechanisms, to the extent permitted by law, to support appropriate private sector screening processes that have a substantial bearing on homeland security;

(d) host mechanisms, to the extent permitted by law, to support appropriate foreign government screening processes that have a substantial bearing on homeland security;

(e) provide or make accessible appropriate information to foreign governments cooperating with the United States in the war on terrorists of global reach; and

(f) ensure that these activities are carried out in a manner consistent with the Constitution and applicable laws. (U)

### Terrorist Screening Center

- (3) To implement the President's directive, the Attorney General, acting through the Director of the FBI, and in coordination with the Secretary of State, the Secretary of Homeland Security, and the Director of Central Intelligence, will establish the Terrorist Screening Center to consolidate the Government's approach to terrorism screening and provide for the appropriate and lawful use of Terrorist Information, in screening processes. (U)
- (4) The Terrorist Screening Center will:
- (a) maintain a consolidated terrorist screening database that is a continuously updated, sensitive but unclassified subset of the Terrorist Information possessed by the TTIC, and the Purely Domestic Terrorism Information (i.e., information about U.S. persons that has been determined to be purely domestic terrorism information with no link to foreign intelligence, counterintelligence, or international terrorism) possessed by the FBI;
  - (b) determine, for each entry in the consolidated terrorist screening database, which supported screening processes shall query that entry, as described in paragraphs (15) through (24);
  - (c) ensure, consistent with applicable law, that appropriate information possessed by State, local, territorial, and tribal governments, which is available to the Federal government, is considered in determinations made by the Terrorist Screening Center;
  - (d) host mechanisms to support appropriate screening processes; and
  - (e) provide continual operational support to assist in the identification of persons screened and, when an individual known or appropriately suspected to be involved in activities constituting, in preparation for, in aid of, or related to terrorism, has been identified through a screening process, facilitate, to the extent permitted by law, appropriate and lawful actions to be taken by appropriate departments and agencies. (U)
- (5) The Terrorist Screening Center will be headed by a senior U.S. Government official (the Director of the Terrorist Screening Center), who will report to the Attorney General through the Director of the FBI. The Director of the Terrorist Screening Center will be appointed by the Attorney General, in consultation with the Secretary of Homeland Security, the Secretary of State, the Director of the FBI, and the Director of Central Intelligence. The Principal Deputy Director of the Terrorist Screening Center will be a senior official from the Department of Homeland Security. (U)
- (6) The Terrorist Screening Center will be staffed with assignees and other officials from the Department of State, the Department of Justice, the Department of Homeland Security, and other Federal departments and agencies that the Terrorist Screening Center supports. The Director of Central Intelligence, acting in his capacity as statutory head of the Intelligence Community, may

also determine that assignees of other appropriate agencies, within the Intelligence Community, will be made available to perform appropriate duties at the Terrorist Screening Center. (U)

(7) Personnel assigned to the Terrorist Screening Center will have appropriate access to the TTIC database and any relevant intelligence information necessary to perform the Terrorist Screening Center's functions. To the extent required by law, the Parties to this Memorandum may jointly determine the circumstances under which personnel from the Intelligence Community, assigned to the Terrorist Screening Center in accordance with paragraph (6), may participate in the functions of the Terrorist Screening Center relating to U.S. persons. (U)

(8) The Director of the Terrorist Screening Center will establish necessary procedures and safeguards to ensure the Terrorist Screening Center's functions are carried out in a manner consistent with the Constitution and applicable laws, including, but not limited to, procedures to:

- (a) address the repeated misidentification of persons in any U.S. Government screening process;
- (b) regularly review information, and to promptly adjust or delete erroneous or outdated information; and
- (c) protect personal privacy. (U)

(9) Consistent with the President's directive, the Secretary of State, in consultation with the Secretary of Homeland Security, the Attorney General, and the Director of Central Intelligence, and working with the Director of the Terrorist Screening Center, not later than 180 days from today, will recommend to the President through the Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs, a proposal for cooperating with certain foreign governments (beginning with those countries for which the United States has waived visa requirements) to establish appropriate access to terrorist screening information of the participating governments, in a manner consistent with each government's laws, and to provide operational support to the participating governments. (U)

#### **Terrorist Threat Integration Center (TTIC) Identities Database**

(10) The TTIC database will include, to the extent permitted by law, all information the U.S. government possesses related to the identities of individuals known or appropriately suspected to be or have been involved in activities constituting, in preparation for, in aid of, or related to terrorism, with the exception of Purely Domestic Terrorism Information. (U)

(11) As directed by the President, and to the extent permitted by law, Federal departments and agencies will provide to the TTIC on an ongoing basis all relevant Terrorist Information in their possession, custody, or control, with the exception of Purely Domestic Terrorism Information, which will instead be provided directly to the FBI. Departments and agencies will continue to



provide new or updated information, and adjust or retract information as needed, in as near to real-time as possible. To this end, the Parties to this Memorandum will automate, to the maximum extent possible while providing for necessary review, their processes and mechanisms for securely sharing this information, including, but not limited to, the following:

(a) The Secretary of State, the Attorney General, the Secretary of Homeland Security, and the Director of Central Intelligence, in coordination with other relevant department and agency heads, not later than 180 days from today, will jointly recommend to the President through the Assistant to the President for Homeland Security, in consultation with the Assistant to the President for National Security Affairs, improvements, if any, to the existing cable-based system of sharing terrorism-related information with other departments and agencies.

(b) The Attorney General will ensure that the FBI's information technology modernization programs incorporate automated means of sharing appropriate information with the TTIC and other departments and agencies, while providing for necessary review, in near real-time. (U)

(12) The TTIC identities database, and the FBI's database containing Purely Domestic Terrorism Information, will incorporate, to the extent permitted by law, available biometric data, including data on persons who even if otherwise unidentified are known or appropriately suspected to be or have been involved in activities constituting, in preparation for, in aid of, or related to terrorism. The databases will have the capability of periodically incorporating advancements in biometric technology. (U)

#### **Relationship of the TTIC and FBI Databases to the Terrorist Screening Center Terrorist Screening Database**

(13) The TTIC identities database will serve, with the exception described in paragraph (10), as the single source for the Terrorist Screening Center terrorist screening database. The Director of the FBI will serve as the source for the Terrorist Screening Center terrorist screening database with regard to Purely Domestic Terrorism Information. The Terrorist Screening Center terrorist screening database will be a continuously updated, sensitive but unclassified subset of the Terrorist Information possessed by the TTIC, and the Purely Domestic Terrorism Information possessed by the FBI. (U)

#### **Terrorist Screening Center Terrorist Screening Database**

(14) The Director of the TTIC, the Director of the Terrorist Screening Center, and the heads of Federal departments and agencies, or their designees, may nominate persons for inclusion in the terrorist screening database, with notification, as appropriate, to the Director of the TTIC and/or the Director of the FBI. (U)

(15) The Terrorist Screening Center will determine, according to criteria established jointly with the entity responsible for each supported screening process, which supported screening processes will query that entry in the consolidated terrorist screening database. The Terrorist Screening Center will make these determinations based on criteria and procedures developed in coordination with the Parties to this Memorandum and in consultation with the heads of appropriate Federal departments and agencies, based on factors including, but not limited to, the following:

- (a) the nature of the person's association with terrorism;
- (b) the quality of the data, including credibility, reliability, and extent of corroboration;
- (c) the extent of uniquely identifying data;
- (d) the authority or authorities under which the data was obtained, and any restrictions on how it may be shared or used;
- (e) the authority or authorities of the screening entity;
- (f) the circumstances, including changes in the Homeland Security Alert Level, under which screening will occur; and
- (g) the action the screening entity will take if a person is identified as a person in the terrorist screening database. (U)

(16) The Director of the Terrorist Screening Center, in coordination with the Parties to this Memorandum and in consultation with the heads of appropriate Federal departments and agencies, will establish procedures to review the continued inclusion of a person in the terrorist screening database, and to review the inclusion of that person in particular screening processes as described in paragraph (15) above, whenever new information about that person is developed. (U)

(17) Except upon written direction from the President, determinations to include U.S. persons in the terrorist screening database based solely on information concerning the domestic activities of such persons will be made as appropriate by the Secretary of State, the Attorney General, and the Secretary of Homeland Security, or their designees. (U)

(18) The Attorney General, acting through the Director of the Terrorist Screening Center, will review each nomination and determine whether to include that person in those records that can be queried by law enforcement authorities through the NCIC database; for aliens, the Attorney General will do so in consultation with the Secretary of Homeland Security, acting through the Secretary of Homeland Security's representative assigned to the Terrorist Screening Center. (U)

(19) The Secretary of Homeland Security, acting through his representative assigned to the Terrorist Screening Center, will review each nomination and determine whether to include that person in those records that can be queried by, or made accessible by appropriate means, to other State, local, territorial, and tribal officials for homeland security purposes, including, but not limited to, screening persons when they apply for driver's licenses or other forms of identification. (U)

(20) The Secretary of Homeland Security, acting through his representative assigned to the Terrorist Screening Center, will review each nomination and determine whether to include that person in those records that will be subject to queries submitted by appropriate private sector critical infrastructure operators or organizers of large events. The Secretary of Homeland Security, in consultation with the other Parties to this Memorandum, and working with the Director of the Terrorist Screening Center, will establish necessary guidelines and criteria to:

(a) govern the mechanisms by which private sector entities can submit such queries; and

(b) initiate appropriate law enforcement or other governmental action, if any, when a person submitted for query by a private sector entity is identified as a person in the terrorist screening database. (U)

(21) The Secretary of State in consultation with the Attorney General, the Secretary of Homeland Security, and the Director of Central Intelligence, acting through their representatives assigned to the Terrorist Screening Center, will review each nomination and determine whether to include that person in those records that can be queried by, or made accessible by appropriate means to, foreign governments cooperating with the United States in the war on terrorists of global reach. (U)

[Paragraphs (22) – (24) are classified and therefore redacted]

(25) The terrorist screening database will be accessible to screening processes on a real-time basis. Screening processes will only be able to access those records that have been identified and approved for such screening, as described in paragraphs (15) through (24) above. The Director of the Terrorist Screening Center will strictly limit, to the maximum extent possible, the need to provide U.S. Government terrorist screening data in list form to supported entities. (U)

#### **Additional Implementation Provisions**

(26) Per the President's direction, and consistent with guidelines developed by the Attorney General in coordination with the other Parties to this Memorandum, the heads of Federal departments and agencies will conduct screening using the Terrorist Screening Center database at all appropriate opportunities, and shall report to the Attorney General not later than 90 days

from today the screening opportunities at which such screening shall and shall not be conducted. (U)

(27) The Attorney General and the Secretary of Homeland Security will conduct a review of the organization, structure and progress of the Terrorist Screening Center at an appropriate time, and report to the President through the Assistant to the President for Homeland Security. The report will include a recommendation on whether any modifications to the Terrorist Screening Center should be made. (U)

(28) To the extent permitted by law, the Director of the TTIC will promptly assume responsibility for the functions and personnel of the Department of State's TIPOFF counterterrorist program, less those components devoted to providing operational support to TIPOFF users and will ensure that all terrorist identity information contained within the TIPOFF database is fully integrated into the TTIC database. The functionality of the TIPOFF program, whereby consular officials receive near real-time feedback to hits to TIPOFF entries, will be maintained or improved upon. A separate Annex to this Memorandum will be promptly agreed to regarding the modalities of TIPOFF relocation to the TTIC, and the specific responsibilities of each party. (U)

(29) Beginning with the standup of the Terrorist Screening Center, Federal departments and agencies will discontinue or transfer to the Terrorist Screening Center, to the extent permitted by law and with appropriate consultation with the Congress, those operations that are duplicative of the Terrorist Screening Center's mission to provide continuous operational support to users of the terrorist screening database, including but not limited to:

(a) those components of the Department of State's TIPOFF counterterrorist program devoted to providing operational support to TIPOFF users (with the exception of a small element that will remain at the Department of State to facilitate intelligence support to the Bureau of Consular Affairs);

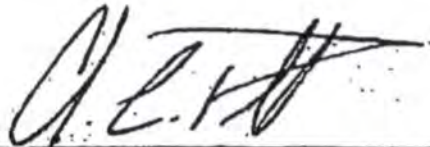
(b) the FBI's Watchlist Unit; and

(c) the Transportation Security Agency's No-Fly and Selectee list program. (U)

(30) Consistent with HSPD-6 and other presidential directives, this Memorandum does not alter existing authorities or responsibilities of the heads of Federal departments and agencies to carry out operational activities or provide or receive information. (U)

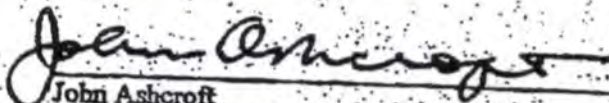
(31) To the extent that existing notices are not sufficient, the Parties to this Memorandum, which will provide information to the TTIC, the FBI, and/or the Terrorist Screening Center under HSPD-6 and this Memorandum, will publish in the Federal Register, prior to the standup of the Terrorist Screening Center, "routine use" notices under the Privacy Act sufficient to indicate that such information will be provided. (U)

(32) This Memorandum of Understanding is effective from the date of signature by all Parties. Any Party may submit, through the Assistant to the President for Homeland Security, written requests for revisions, amendments, modifications, annexes and supplementary understanding to this Memorandum at any time. Such changes shall become effective upon the date of approval by all Parties. The Parties shall review this Memorandum not later than one year from its effective date. (U)



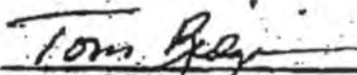
Colin L. Powell  
Secretary of State

September 16, 2003



John Ashcroft  
Attorney General

September 16, 2003



Thomas J. Ridge  
Secretary of Homeland Security

*Sept. 16, 2003*  
September 16, 2003



George J. Tenet  
Director of Central Intelligence

September 16, 2003

Signatures are consolidated from classified version of the original TSC MOU.

**THE SECRETARY OF STATE  
THE SECRETARY OF THE TREASURY  
THE SECRETARY OF DEFENSE  
THE ATTORNEY GENERAL  
THE SECRETARY OF HOMELAND SECURITY  
THE DIRECTOR OF NATIONAL INTELLIGENCE  
THE DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY  
THE DIRECTOR OF THE NATIONAL COUNTERTERRORISM CENTER  
THE DIRECTOR OF THE TERRORIST SCREENING CENTER**

**ADDENDUM B**

**TO THE  
MEMORANDUM OF UNDERSTANDING ON THE INTEGRATION AND USE OF  
SCREENING INFORMATION TO PROTECT AGAINST TERRORISM**

**Background**

(1) This Addendum, ("Addendum B") supplements the Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism, dated September 16, 2003, ("the TSC MOU") and supercedes Addendum A, effective August 2, 2004. To the extent that Addendum B is inconsistent with the TSC MOU, Addendum B supercedes the TSC MOU. In addition, Addendum B supercedes the TIPOFF-TERROR Memorandum of Understanding, dated June 4, 2002, between the Department of State, the Defense Intelligence Agency, the National Security Agency, the Federal Bureau of Investigation, and the Central Intelligence Agency or any other interim agreement intended to address the use of disseminated Terrorism Information.

(2) Addendum B incorporates by reference all provisions of the Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing, dated March 4, 2003 ("the Information Sharing MOU") and the TSC MOU. By their signatures on Addendum A, the Secretary of State, the Secretary of the Treasury, and the Secretary of Defense became signatories of the Information Sharing MOU and the TSC MOU and agree that all provisions of those MOUs apply to all entities that are, or become, wholly or in part, part of, respectively, the Department of State, the Department of the Treasury and the Department of Defense. To the extent that the TSC MOU and Addendum B provide for greater information sharing than that mandated by the Information Sharing MOU, the provisions of the TSC MOU and Addendum B shall control the Parties' actions. In all other respects, to the extent that provisions of the TSC MOU and/or Addendum B are inconsistent with the Information Sharing MOU, the provisions of the Information Sharing MOU shall control the actions of the Parties to this Addendum.

**Purpose**

(3) The purposes of Addendum B are:

(a) to ensure the full implementation of subparagraph (2) of Homeland Security Presidential Directive-6 (HSPD-6), dated September 16, 2003, entitled "Integration and Use of Screening Information to Protect Against Terrorism;" and

(b) to memorialize the Parties' agreement that they will, to the maximum extent permitted by law and consistent with the President's direction for the establishment of the Terrorist Threat Integration Center, now the National Counterterrorism Center (NCTC) and the Information Sharing MOU, provide to the NCTC on an ongoing basis all Terrorism Information (as defined in the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, Section 1016(a)(4)) in their possession, custody, or control.

#### Procedures

(4) The Parties will, to the maximum extent permitted by law and consistent with the establishment of the NCTC, the Information Sharing MOU, and in furtherance of the information sharing mandates in IRTPA, provide to the NCTC, on an ongoing basis, all Terrorism Information, in their possession, custody, or control. If additional procedures and mechanisms are needed beyond those directed in the Information Sharing MOU and IRTPA to accomplish this including, but not limited to, compartmented programs, the NCTC, in coordination with the Parties disseminating the Terrorism Information ("Originators"), shall establish procedures to guide the provision of such information, and the Parties shall establish procedures and mechanisms to provide such information.

(5) A web-based version of the NCTC Identities Database, the Terrorist Identities Datamart Environment (TIDE-Online), as mandated in the TSC MOU, will be available to all individuals who have obtained an IC certificate for access to NCTC Online (NOL), formerly known as CTLINK, which is a Community of Interest on INTELINK. The NCTC will make available to the Parties upon request, the names and clearances of personnel with access to TIDE-Online. All users will be responsible for complying with the conditions set for access to TIDE-Online.

(6) When the Parties provide disseminated Terrorism Information to the NCTC, no specific notification will occur between the NCTC and the Originator identifying the fact that Terrorism Information contained in those communications were placed in TIDE.

(7) The Parties authorize the NCTC (and the FBI for Purely Domestic Terrorism Information, as defined in the TSC MOU) to provide to the TSC the following data (referred to as, "Terrorist Identifiers"), in accordance with the provisions of paragraph (8) below, for inclusion in the TSC's consolidated terrorist screening database (TSDB):

- (a) Names and aliases;
- (b) Dates of birth;
- (c) Places of birth;
- (d) Unique identifying numbers such as alien registration numbers, visa numbers, social security account numbers;
- (e) Passport information, including passport numbers, countries of issuance, dates and locations of issuance, expiration dates, passport photos, and other relevant data;
- (f) Countries of origin and nationalities;

- (g) Physical identifiers, such as sex, race, height, weight, eye color, hair color, scars, marks, or tattoos;
- (h) Known locations, i.e. addresses;
- (i) Photographs or renderings of the individual;
- (j) Fingerprints or other biometric data;
- (k) Employment data;
- (l) License plate numbers;
- (m) Any other Terrorism Information that Originators specifically provide for passage to the TSC.

(8) Once provided to the NCTC (or the FBI for Purely Domestic Terrorism Information), the Parties agree that the NCTC (or the FBI for Purely Domestic Terrorism Information) will deem the Terrorist Identifiers listed in paragraph (7) For Official Use Only (FOUO) for the purposes of providing the data to the TSC for inclusion in TSDB. These Terrorist Identifiers passed to the TSC and retained in TSDB will be deemed FOUO.

(9) The Originator may prohibit the NCTC from passing the Terrorist Identifier(s) identified in (a) – (m) above to the TSC as FOUO data for inclusion in TSDB if an appropriate official so authorizes. Each Originator shall identify its Terrorist Identifier(s) that are to be prohibited from being passed to the TSC for inclusion in TSDB by marking those items, "TIDE restricted." Restrictions on use shall be imposed only to the extent strictly necessary to prevent the unauthorized disclosure of information that clearly identifies, or would reasonably permit ready identification of, intelligence or sensitive law enforcement sources, methods, activities or cryptology that are particularly susceptible to countermeasures that would nullify or measurably reduce their effectiveness.

(10) The Parties agree that subject to an Originator's ability to prohibit specific Terrorist Identifiers from being included in TSDB, all Terrorist Identifiers listed in (7) may be passed to the TSC, regardless of the date or classification of the disseminated Terrorism Information.

(11) Nothing in Addendum B shall inhibit or delay the provision of Terrorism Information to the NCTC.

(12) Absent prior approval by the Originator, information (including all information designated classified or FOUO in TIDE and information in TSDB) may not be used in any legal or administrative proceeding or process, including any judicial or quasi-judicial process, presentation to grand or petit juries, submission as part of an application for subpoenas, orders for electronic surveillance, search or arrest warrants, presentation as evidence, or any use that could result in public disclosure. Information from FISA collection, or derived therefrom may only be used in legal or administrative proceeding or process with the advance authorization of the Attorney General. Any recipient of information from TSDB interested in obtaining authorization to use that information in a legal or administrative proceeding or process must contact the TSC to obtain the approval of the Originator. If TSDB information is from FISA collection, or derived therefrom, the TSC through FBI Headquarters, will obtain the necessary



Attorney General authorization. Any reproduction, dissemination, or communication (including, but not limited to, oral briefings) of any information from TSDB must be accompanied by a statement of these restrictions. Nothing in this paragraph shall inhibit the sharing of a limited set of Terrorist Identifiers: name; date of birth; passport number; passport country of origin/citizenship, with state, local and tribal authorities, or foreign governments for terrorism screening purposes, as permitted by law, regulation, or agreement of the Parties.

(13) When an individual in TSDB has been positively identified during a screening encounter, the Parties will provide the NCTC with Terrorism Information collected during the encounter, such as photographs, fingerprints, copies of pocket litter, copies of written data, any reports of Terrorism Information provided by that individual, or other items of potential interest, for inclusion in TIDE. The NCTC and/or the TSC will, in partnership with departments and agencies which are not Parties to Addendum B, but which conduct screening using TSDB, establish procedures to ensure that, when an individual in TSDB has been positively identified during a screening encounter, those departments and agencies will provide the NCTC and all appropriate agencies that have a counterterrorism mission, with Terrorism Information as described above.

(14) The Director of the TSC shall establish procedural safeguards, including, but not limited to, training, standard operating procedures, and caller authentication procedures, and shall implement technological safeguards, including, but not limited to, the use of firewalls and public key encryption, to minimize the unauthorized disclosure of information, and to reduce the vulnerability of TSDB to unauthorized access or exploitation. The establishment of these safeguards shall in no way inhibit or delay the provision of information to the NCTC or the TSC.

(15) Addendum B amends Director of Central Intelligence Directive 2/4 (DCID 2/4) by replacing the term "terrorist threat-related information," wherever it appears in DCID 2/4, with the term Terrorism Information, as defined in the IRTPA.

#### Implementation

(16) Addendum B is effective from the date of signature by all Parties and applies to all disseminated Terrorism Information, regardless of the date of the document in which it is contained. Addendum B may be signed in counterparts.

(17) The NCTC, the TSC, and the Parties, in coordination with appropriate Originators, shall report to the Homeland Security Advisor from time to time as appropriate, on the progress made to implement Addendum B.

(18) Nothing in Addendum B alters, or impedes the ability or authority of federal departments and agencies to perform their responsibilities under law, consistent with applicable legal authorities and Presidential guidance. Specifically, nothing in Addendum B alters the information sharing requirements of the Homeland Security Act or the requirements of the IRTPA.

*Condoleezza Rice*

MAY 4 2006

Secretary of State

Date

Secretary of the Treasury

Date

Secretary of Defense

Date

Attorney General

Date

Secretary of Homeland Security

Date

Director of National Intelligence

Date

Director, Central Intelligence Agency

Date

*Andrew Ross*

Mar 30, 2006

Director, National Counterterrorism Center

Date

*John Bell*

April 30, 2006

Director, Terrorist Screening Center

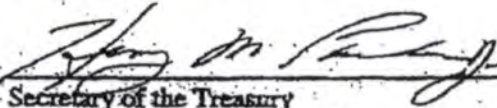
Date

APR. 3. 2006 2:10PM

NO. 136 P. 6

Appendix 4

Secretary of State Date

 Jan 19, 2007  
Secretary of the Treasury Date

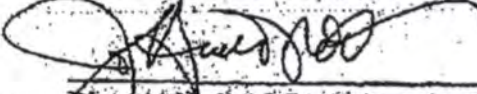
Secretary of Defense Date

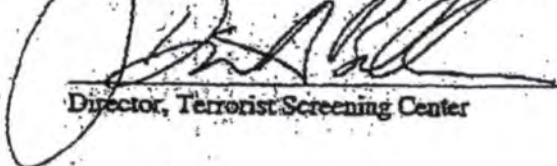
Attorney General Date

Secretary of Homeland Security Date

Director of National Intelligence Date

Director, Central Intelligence Agency Date

 Mar 30, 2006  
Director, National Counterterrorism Center Date

 April 30, 2006  
Director, Terrorist Screening Center Date

Secretary of State Date

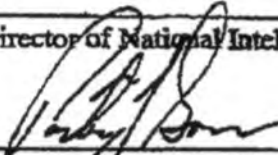
Secretary of the Treasury Date

Secretary of Defense Date

Attorney General Date

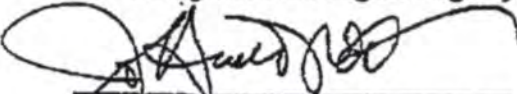
Secretary of Homeland Security Date

Director of National Intelligence Date




27 April 2006

Director, Central Intelligence Agency Date



Mar 30, 2006

Director, National Counterterrorism Center Date



April 30, 2006

Director, Terrorist Screening Center Date

Secretary of State Date

Secretary of the Treasury Date

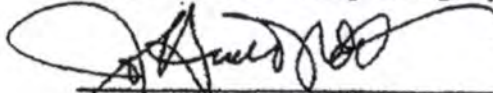
Secretary of Defense Date

Attorney General Date

Secretary of Homeland Security Date

  
Director of National Intelligence Date  
*April 7, 2006*

Director, Central Intelligence Agency Date

  
Director, National Counterterrorism Center Date  
*Mar 30, 2006*

  
Director, Terrorist Screening Center Date  
*April 30, 2006*

R-18-2006 18:49  
APR. 3.2006 1:08PM

NO.135 P.6

Appendix 4

Secretary of State Date

Secretary of the Treasury Date

Secretary of Defense Date

Attorney General Date

Secretary of Homeland Security Date

Director of National Intelligence Date

Director, Central Intelligence Agency Date

Director, National Counterterrorism Center Date

Director, Terrorist Screening Center Date

*April 10, 2006*

*Mar 30, 2006*

*April 30, 2006*

Secretary of State Date

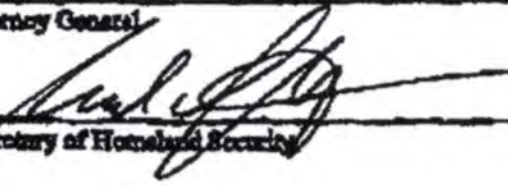
Secretary of the Treasury Date



NOV 9 2006

Secretary of Defense Date

Attorney General Date

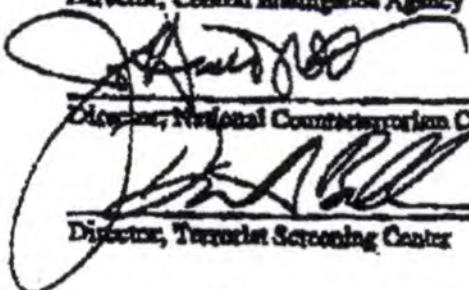


April 10, 2006

Secretary of Homeland Security Date

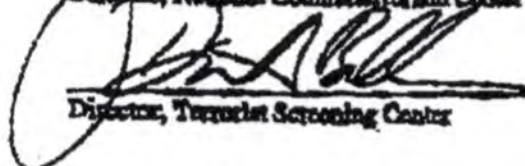
Director of National Intelligence Date

Director, Central Intelligence Agency Date



Mar 30, 2006

Director, National Counterterrorism Center Date



Apr 30 2006

Director, Terrorist Screening Center Date

DAC-01104-03

Appendix 5



UNCLASSIFIED//FOR OFFICIAL USE ONLY  
THE DIRECTOR OF CENTRAL INTELLIGENCE  
WASHINGTON, D.C. 20505

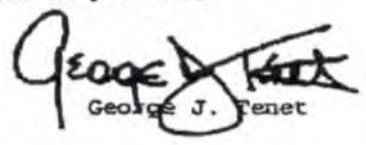
DAC-91355-03  
4 March 2005

MEMORANDUM FOR: National Foreign Intelligence  
Program Principals  
SUBJECT: (U//FOUO) Homeland Security Information  
Sharing Memorandum of Understanding

1. (U//FOUO) The Attorney General, Secretary of Homeland Security, and I have just signed the attached Memorandum of Understanding on Information Sharing (MOU) implementing information sharing requirements of the Homeland Security Act (Act). It is effective immediately. As you know, the Department of Homeland Security (Department) has now reached critical mass. Our corresponding intelligence support function has also matured.

2. (U//FOUO) As with much recent homeland security-related work, the drafting process on this high priority White House initiative moved quickly. Successive drafts were sent to each of your agencies, with all comments forwarded directly to the White House drafting team. The resulting MOU is a fair expression of what the Act requires. I expect each of you to hold those you supervise accountable for giving full effect to each of the MOU's provisions. Note that the MOU makes Associate Director of Central Intelligence for Homeland Security, Winston P. Wiley my representative for information sharing under the MOU. He has my proxy and full support.

3. (U//FOUO) Full and efficient implementation of the MOU will benefit not only the Department, but also intelligence and law enforcement agencies. As with the Terrorist Threat Integration Center, we will embrace the opportunities and challenges it presents.

  
George J. Tenet

cc: ADCI/HS, Winston P. Wiley

Attachment:  
MOU on Information Sharing

UNCLASSIFIED//FOR OFFICIAL USE ONLY



MEMORANDUM OF UNDERSTANDING BETWEEN THE INTELLIGENCE  
COMMUNITY, FEDERAL LAW ENFORCEMENT AGENCIES, AND THE DEPARTMENT  
OF HOMELAND SECURITY CONCERNING INFORMATION SHARING

This Agreement provides a framework and guidance to govern information sharing, use, and handling between: the Secretary of Homeland Security, on behalf of the Department of Homeland Security (DHS), including all entities that are or become, wholly or in part, elements of DHS; the Director of Central Intelligence (DCI), on behalf of all entities that are, or become, wholly or in part, elements of the United States Intelligence Community (IC), other than those that are to become part of DHS; and the Attorney General, on behalf of the Department of Justice (DOJ), including the Federal Bureau of Investigation, and all entities that are, or become, wholly or in part, elements of DOJ, and any other department, agency, or entity having federal law enforcement responsibilities, other than those that are to become part of DHS.

I. Scope of Application. This Agreement shall be binding on all such departments, agencies, and entities on whose behalf the Secretary of Homeland Security, the DCI, and the Attorney General agree herein. This Agreement is intended to mandate minimum requirements and procedures for information sharing, use, and handling, and for coordination and deconfliction of analytic judgments. Departments and agencies are encouraged to develop additional procedures and mechanisms to provide for greater information sharing and coordination than required herein, consistent with the DHS Legislation and other relevant statutory authorities, Presidential Directives, the President's announced policies for protecting against terrorist threats to the homeland, and this Agreement, including, but not limited to:

- (a) the Homeland Security Act of 2002;
- (b) the National Security Act of 1947, as amended;
- (c) the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001;
- (d) the Foreign Intelligence Surveillance Act, as amended;
- (e) Executive Order 12333, as amended, and any subsequent Executive Orders on Intelligence Activities;
- (f) Executive Order 13231, as amended, and any subsequent Executive Orders on Homeland Security;
- (g) Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation, dated September 23, 2002; and
- (h) Guidelines for Disclosure of Grand Jury and Electronic Wire, and Oral Interception Information Identifying United States Persons, dated September 23, 2002.

To the extent that this Agreement provides for more expansive information sharing than other authorities or agreements, with the exception of statutes, or Presidential Directives including, but not limited to, Executive Orders, ("Presidential Directives"), the more expansive provisions of this Agreement shall be followed

2. Definitions. For purposes of this Agreement:

(a) "Analytic conclusion" means the product of analysis of one or more pieces of information in which inferences are drawn from the information being analyzed to arrive at a determination about a fact – such as, for example, a potential threat – that is not explicit or apparent from the face of the original information itself. It does not include, for example, a summary of the factual content of a piece of intelligence information, a report of an interview, or a report or other document that merely collects and summarizes information from multiple sources about the same or related topics, or other types of communication which do not include analytic conclusions as described above.

(b) "Attorney General" means the Attorney General of the United States or the Attorney General's designee, except as otherwise provided herein.

(c) "Classified information" means information that has been determined pursuant to Executive Order No. 12958, or any successor order, Executive Order No. 12951, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure.

(d) "Covered entity" means: any department, agency, bureau, office or other entity that is, or becomes, wholly or in part, an element of the Department of Homeland Security (including the Department itself); any department, agency, bureau, office or other entity that is, or becomes, wholly or in part, an element of the United States Intelligence Community or the Department of Justice; and any other department, agency, or entity having federal law enforcement responsibilities.

(e) "Covered information" means terrorism information, weapons of mass destruction (WMD) information, vulnerabilities information, and other information relevant to the duties of the Department of Homeland Security, as well as analyses based wholly or in part on such covered information.

(f) "Department" or "DHS" shall mean the Department of Homeland Security and any entity that is, or becomes, an element of that Department.

(g) "DHS Legislation" means the Homeland Security Act of 2002 (H.R. 5005, 107th Congress, 2d Session) (November 26, 2002), as it may be amended from time to time.

(h) "DCI" means the Director of Central Intelligence, or, except as otherwise provided herein, the DCI's designee, in his or her capacity as head of the Intelligence Community, and as head of the Central Intelligence Agency.

(i) "Foreign intelligence" has the meaning given to that term in section 3 of the National Security Act of 1947, as amended (50 U.S.C. 401a), as that statutory term may be amended from time to time.

(j) "Homeland" means the United States as defined in the DHS Legislation.

(k) "Infrastructure" means the basic systems, assets, facilities, services, and installations needed for the functioning of our society. The term includes, but is not limited to, critical infrastructure, meaning systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on United States national security, economic security, national public health or safety, or any combination of these. Critical infrastructure includes, but is not limited to, agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry and hazardous materials, postal and shipping, and national monuments and icons.

(l) "Infrastructure information" means all information related to the identification, status, security, criticality, risk assessment, vulnerability to all means of attack, interdependency, and attack consequences (including potential impact on public health or safety, the economy, national security, governance and public confidence) of the infrastructure of the United States.

(m) "Intelligence Community" has the meaning given it in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)), as it may be amended from time to time.

(n) "Need-to-know" means a determination made by an authorized holder of classified information, or sensitive law enforcement information, that a prospective recipient requires access to a specific piece, or category of information in order to perform or assist in a lawful and authorized governmental function.

(o) "Parties" means the signatories to this Agreement and their successors, on behalf of all covered entities they head, supervise or represent.

(p) "PATRIOT Act" means the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. 107-56, 115 Stat. 272, 278-81.

(q) "Secretary" means the Secretary of Homeland Security or the Secretary's designee, except as otherwise provided herein.

(r) "Terrorism information" means all information relating to the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, domestic groups or individuals involved in terrorism, to threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations, or to communications between such groups or individuals, and to

information relating to groups or individuals reasonably believed to be assisting or associated with them.

(s) "Vulnerabilities information" means all information relating to the susceptibility – actual, perceived, or conceptual – of the United States, including any portion, sector, population, geographic area, or industry, to terrorist attack.

(t) "Weapons of Mass Destruction information" or "WMD information" means terrorism information or vulnerabilities information relating to conventional explosive weapons and non-conventional weapons capable of causing mass casualties and damage, including chemical or biological agents, radioactive or nuclear materials, and the means to deliver them.

3. Policies and Procedures for Information Sharing, Handling and Use. Consistent with the DHS Legislation, and except as otherwise specifically provided in this Agreement, the following agreed-upon policies and procedures shall apply to the provision of covered information by any covered entity to any other covered entity, to the interpretation of all provisions of this Agreement, and to the resolution of all issues related to information sharing, handling and use, and the coordination and deconfliction of operations and analytic conclusions:

(a) *Priority on Preemption, Prevention, and Disruption.* All procedures, guidelines, and mechanisms under this Agreement shall be designed and implemented, and all determinations with regard to sharing information covered by this Agreement shall be made, with the understood, overriding priority of preventing, preempting, and disrupting terrorist threats to our homeland. The parties recognize and agree that, in some cases, this priority shall dictate information sharing even where doing so may affect criminal prosecutions or ongoing law enforcement or intelligence operations. Nonetheless, the covered entities shall act under this Agreement in a manner to protect, to the greatest extent possible, these other significant interests, including the protection of intelligence and sensitive law enforcement sources and methods, other classified information, and sensitive operational and prosecutorial information.

(b) *Reciprocity and Transparency.* All information collected by any covered entity relevant to the missions and responsibilities of any other covered entities should be shared, to the greatest extent possible, between and among all covered entities. Likewise, the parties agree that, to the greatest extent possible, there should be transparency between and among the covered entities with regard to their activities to preempt, prevent, and disrupt terrorist attacks against U.S. persons and interests. Except as otherwise specified in this Agreement, or mandated by relevant Federal statutes or Presidential Directives, procedures and mechanisms for information sharing, use, and handling shall be interpreted and implemented consistently and reciprocally regardless of the role a particular covered entity plays as a provider or recipient of covered information. In other words, for example, international terrorism information collected by the Border Patrol should be shared by DHS with the IC to the same extent foreign intelligence information on terrorism is shared by the IC with DHS.

(c) *Scope of "Covered Information."* Consistent with the priority established in Section 3(a), information relating to terrorism, Weapons of Mass Destruction, vulnerabilities, or other functions of the Department of Homeland Security shall be presumed to be "covered information" under this Agreement. If, after applying this presumption, disagreement remains between covered entities about whether particular information is "covered information," such disagreement shall be resolved pursuant to Section 4(d).

(d) *Effective date of information sharing obligations.* Notwithstanding provisions of this Agreement mandating further agreement on mechanisms, procedures, or other issues, the parties recognize that the obligation to promptly begin the full range of information sharing mandated by the DHS Legislation came into force on January 24, 2003, and that obligations under this Agreement will be in force upon the signature of all parties.

(e) *Sharing Requirements Based on Substance Only.* Consistent with the DHS Legislation and other relevant statutory authorities, Presidential Directives, the President's announced policies for protecting against terrorist threats to the homeland, and this Agreement, the parties agree that this Agreement requires that covered information, including, but not limited to, terrorism information, WMD information, infrastructure, and vulnerabilities information, be provided by any covered entity that collects or analyzes that information to any other covered entity that has a need-to-know that information (or information relating to that subject matter), based on a broad interpretation of the mission of the other covered entity, regardless of:

(i) The type of communication in which the information is incorporated. Covered information must be provided as required in this Agreement regardless of the type of communication in which it is originally reported by the providing agency. The fact that particular covered information may be contained originally in a particular type of communication shall not, under any circumstances, be grounds either to withhold or delay the sharing of any covered information. As illustrative examples only, covered information must be provided by CIA, within the time frames agreed to, whether such information is contained originally in communications referred to as "TDs," "intel cables," "ops cables," or any other type of communication. Likewise, covered information must be provided by the FBI, within the time frames agreed to, whether such information is contained originally in communications referred to as "302s," "ECs," "LHMs," or any other type of communication;

(ii) The manner in which the information is or may be conveyed to the intended agency or individual recipients. Covered entities shall continually endeavor to improve technological means of access to afford maximum flexibility, speed, and volume of information shared, consistent with the strictly necessary protection of intelligence or sensitive law enforcement sources and methods, and with section 3(a) and other relevant provisions of this Agreement.

(f) *Terrorist Threat Integration Center.* The parties agree that, when fully operational, the Terrorist Threat Integration Center (TTIC) shall be the preferred, though not the exclusive, method for sharing covered information at the national level. TTIC information-sharing mechanisms and procedures shall be consistent with the DHS Legislation and other relevant statutory authorities, Presidential Directives, the President's announced policies for protecting against terrorist threats to the homeland, and this Agreement. As soon as practicable, the parties shall determine the extent to which provision of information to one or more covered entities via the TTIC may constitute the only required method for providing such information to such entities, *provided however*, that any decision to share covered information among the parties solely by means of the TTIC shall be memorialized in a separate written agreement executed by the parties, including by designees of the officials signing this Agreement. Analytic conclusions contained in TTIC products shall not be altered by agencies prior to dissemination.

(g) *Policies for Sharing Particular Types of Information With DHS.* Consistent with the DHS Legislation and other relevant statutory authorities, Presidential Directives, the President's announced policies for protecting against terrorist threats to the homeland, and this Agreement, the Secretary shall be provided access to all information necessary for him to carry out the mission of the Department. Except as otherwise directed by the President, the parties agree that the amount of information and depth of detail of information provided to the Secretary, which will vary by the type of information at issue, will be governed by the following policies:

(i) Information Related to Threats of Terrorism Against the United States. As required by the DHS Legislation, DHS shall be provided, without request, all "reports (including information reports containing intelligence which has not been fully evaluated), assessments, and analytical information." The parties understand that, in this category, except upon further request by DHS, and agreement by the originating entity, provided information will not routinely include information, collected through intelligence sources or methods, or sensitive law enforcement sources or methods, which has not been processed in any way to reduce the amount of substantive content or synthesize the material. Thus, for example, a recording of a conversation intercepted under the Foreign Intelligence Surveillance Act (FISA) or an intelligence officer's or FBI agent's hand-written notes of a discussion with a source would not be routinely provided in this category. By contrast, a report forwarding the substance of a FISA-recorded conversation, or an FBI "Electronic Communication" (EC), including the substance of a discussion with a source, even if these include verbatim quotes from the underlying notes, would be provided. ECs containing substantive information, along with "302s," "TDs," "IIRs," and all other similar documents including substantive information, fall into the category of information to be provided. The parties agree, as soon as practicable, to identify and/or put into place necessary and reasonable mechanisms, including, when operational, the TTIC, along with the Joint Terrorism Task Forces (JTTFs), and procedures, to ensure that DHS receives all such information automatically, under the policies

and procedures agreed to in this Agreement, without further request.

(ii) Vulnerabilities Information. As required by the DHS Legislation, DHS shall be provided, without request, all information of any kind concerning "the vulnerability of the infrastructure of the United States; or other vulnerabilities of the United States, to terrorism, whether or not such information has been analyzed." The parties understand that, in this category, without further request by DHS, provided information will routinely include information, collected through intelligence sources or methods, or sensitive law enforcement sources or methods, which has not been processed in any way to reduce the amount of substantive content or synthesize the material. Provided information will include all types of information, without regard to the distinctions drawn by way of example in Section 3(g)(i), except as further agreed to by the parties or their designees. The parties agree, as soon as practicable, to identify and/or put into place necessary and reasonable mechanisms, including, when operational, the TTIC, along with the JTTFs, and procedures, to ensure that DHS receives all such information, under the principles agreed to in this Agreement, without further request.

(iii) Information Relating to Significant and Credible Threats of Terrorism. As required by the DHS Legislation, DHS shall be provided, without request, all information of any kind concerning "significant and credible threats of terrorism against the United States, whether or not such information has been analyzed." The parties understand that, in this category, without further request by DHS, provided information will routinely include information, collected through intelligence sources or methods, or sensitive law enforcement sources or methods, which has not been processed in any way to reduce the amount of substantive content or synthesize the material. Provided information will include all types of information, without regard to the distinctions drawn by way of example in Section 3(g)(i), except as further agreed to by the parties or their designees. The parties agree, as soon as practicable, to identify and/or put into place necessary and reasonable mechanisms, including, when operational, the TTIC, along with the JTTFs, and procedures, to ensure that DHS receives all such information, under the principles agreed to in this Agreement, without further request.

(iv) Other Information Requested by the Secretary. The Secretary shall be provided, upon request, with such other information relating to threats of terrorism against the United States or to other areas of DHS' responsibility, whether or not such information has been analyzed. The parties understand that DHS will be provided information in this category upon request including, if so requested, information which has not been processed in any way to reduce the amount of substantive content or synthesize the material. If so requested, provided information will include all types of information, without regard to the distinctions drawn by way of example in Section 3(g)(i), except as otherwise directed by the President. The parties agree, as soon as practicable, to set up

necessary and reasonable mechanisms, including, when operational, the TTIC, along with the JTTFs, and procedures, to ensure that DHS, when requested, receives all such information, under the principles agreed to in this Agreement.

(h) *Timely Sharing of Information.* Covered information must be provided to those with a need-to-know that information (or information relating to that subject matter), based on a broad interpretation of the mission of the other covered entity, as quickly as possible. Providing all timely and relevant covered information to those who have a need-to-know it in order to assist them in meeting their homeland security-related responsibilities is fundamental to the success of the Department and all other efforts to ensure the security of the homeland from terrorist attack. Delay in providing such information risks frustrating efforts to meet these critical responsibilities and could result in preventable attacks against U.S. persons or interests failing to be preempted, prevented, or disrupted. Accordingly, except as otherwise directed by the President or agreed to by all parties, the parties agree that:

(i) Information that a covered entity reasonably believes relates to a potential terrorism or WMD threat, to the United States homeland, its infrastructure, or to United States persons or interests, shall be provided immediately to other covered entities;

(ii) Other covered information, including, but not limited to, vulnerabilities information, but which a covered entity does not reasonably believe relates to a potential terrorism or WMD threat to the United States homeland, its infrastructure, or to United States persons or interests, shall be provided as expeditiously as possible;

(iii) Under no circumstances may covered information be withheld from a covered entity with a need-to-know that information (or information relating to that subject matter), based on a broad interpretation of the mission of the other covered entity, or may the sharing of such information be delayed beyond the time frames agreed to in this Agreement, except as consistent with the Section 4(d), or other relevant provisions of this Agreement;

(iv) When a question arises as to whether covered information must be provided to the Department or any other covered entity pursuant to this Agreement, the parties will resolve the question pursuant to Section 4(d);

(v) Covered entities agree to use, to the greatest extent possible, the most rapid methods of information sharing, consistent with the strictly necessary protection of intelligence or sensitive law enforcement sources and methods, and with Section 3(a) and other relevant provisions of this Agreement; and

(vi) Consistent with Section 3, and other relevant provisions of this Agreement, the parties agree that they shall work diligently to ensure that all covered entities receive the same information within the same time frame,



Agreement, to withhold in its entirety a communication containing covered information, such indication shall occur immediately.

(v) The parties agree that the provisions of this section shall not apply to established source protection procedures utilized by CIA's Directorate of Operations, or equivalent procedures developed and used by other covered entities, *provided that* such procedures do not result in the failure to provide DHS with substantive information as required under the DHS Legislation and this Agreement, and that the Secretary may personally request revisions in such procedures if he determines that they restrict DHS' access to information in a way that jeopardizes DHS' mission. For information described in Section 3(i)(i), such procedures shall be revised, as soon as is practicable, and without request from the Secretary, to ensure that those procedures only remove such intelligence that clearly identifies, or would reasonably permit ready identification of, intelligence or sensitive law enforcement sources or methods that are particularly susceptible to countermeasures that would nullify or measurably reduce their effectiveness.

(j) *Requests for Additional Information.* In addition to the participation of DHS in the "requirements" processes, as discussed further herein, the DHS Legislation provides for DHS to request additional or follow-up information upon receipt of individual items of information. As soon as practicable, the parties shall agree to mechanisms and procedures, including the TTIC, JTTFs, and, if appropriate, focal points, for DHS to make, and covered entities to respond to, such requests. These mechanisms and procedures shall be designed to facilitate the greatest amount of additional information sharing consistent with strictly necessary protection of intelligence or sensitive law enforcement sources and methods, with Section 3(a) and other relevant provisions of this Agreement, and with the timeliest possible responses to requests for additional information.

(k) *Information Use Restrictions.* In general, parties shall disclose covered information free of any originator controls or information use restrictions. Several categories of covered information that must be disclosed to covered entities pursuant to the DHS Legislation, this Agreement, and other authorities, remain subject to special labeling, handling, storage, use and access auditing requirements imposed by statute or, to the extent consistent with the DHS Legislation, Presidential Directives, the President's announced policies for protecting against terrorist threats to the homeland, and this Agreement, pursuant to applicable regulations. The scope and duration of such restrictions, including caveats restricting use of the disclosed information to a particular level or element of a covered entity, will be tailored to address the particular situation or subject matter involved. When imposed, use restrictions shall be no more restrictive than strictly necessary to accomplish the desired effect.

(l) *Secondary Information Sharing.* To the extent consistent with this Agreement, covered entities may share information provided by other covered entities with additional covered entities. Such secondary sharing shall be carried out, to the greatest extent possible, in a manner that permits the originating agency to know to

whom the information has been provided. The parties shall agree, as soon as is practicable, upon recommendations, if any, for changes to Executive Order 12958, Director of Central Intelligence Directive 6/6 (and complementary or successor directives dealing with Originator Controls, the so-called "third agency rule," and other policies or procedures governing the sharing of received information with additional recipients) in order to comply with the DHS Legislation, and to carry out the President's announced policies for protecting against terrorist threats to the homeland, and the provisions of this Agreement.

(m) *Other Obligations to Share Information.* A covered entity's voluntary or obligatory provision of covered information to another covered entity does not in itself discharge or diminish any other obligation the providing entity may have to provide that information, or any part of it, to any other department, agency or other public or private organization or individual under any statute, Presidential Directive, or other agreement. Although all covered entities will attempt to identify and call attention to information relevant to the mission of other covered entities, the responsibility to share information relevant to the mission or responsibilities of any covered entity in addition to DHS remains the responsibility of the originator or initial federal recipient of the information and does not shift to DHS by virtue of DHS' receipt of the information. The parties agree, however, that, to the greatest extent possible, other sharing obligations shall be harmonized and coordinated with those covered by this Agreement, including the agreed preference for using the TTIC and JTTFs as information-sharing mechanisms, in order to reduce duplication, facilitate deconfliction, and increase efficiency.

(n) *PATRIOT Act Information.* Law enforcement-related information related to DHS mission, permitted or required to be provided to intelligence agencies under the PATRIOT Act and its implementing guidelines shall also be considered covered information under this Agreement and shall, therefore, be provided to the Department and other covered entities, in accordance with the DHS Legislation and other relevant statutory provisions, and this Agreement.

(o) *Other Intelligence Information.* Nothing in this Agreement shall be read to restrict the access of the Secretary or his designee to information the Secretary ordinarily would receive as a member of the Intelligence Community, including national security and foreign intelligence information.

(p) *Information Sharing Mechanisms.* As soon as practicable, the parties shall agree upon specific mechanisms, consistent with Section 3 and other relevant provisions of this Agreement, for how different types of covered information will be shared, including technical and administrative arrangements, and, as appropriate, designation of focal points, to maximize the effectiveness and coordination for providing covered information. Subsequent arrangements for information sharing may be reached upon the approval of the parties or their designees. The parties shall work to develop, as part of this process, effective mechanisms for covered entities to identify covered information held by them and to ensure, to the greatest degree feasible, the provision of such information, without specific request, to other covered entities. The parties further agree

that, notwithstanding their agreement to develop further mechanisms and procedures for information sharing, covered entities shall promptly build on mechanisms and procedures already in place to identify and provide to DHS covered information that is generated or received by them in the course of carrying out their missions.

(q) *Methods of Providing Information.* The parties recognize and agree that there are many possible methods for "providing" information, including, but not limited to, hand-delivery, oral briefings, transmission by secure data-link, and affording routine and unrestricted access to computerized databases, including the ability to transfer such information to a recipient entity as necessary, and by full and complete co-location of analysts or other personnel and full integration of, and access to, information, as well as, for example, ensuring that the Secretary receives all daily threat briefing materials (including threat matrices and overnight reports). The parties further agree that requirements to "provide" information under this Agreement may be satisfied, depending on the type of information at issue, by the use of a single mechanism, such as via the TTIC, consistent with section 3(f) of this Agreement, or a combination of mechanisms already in place and/or created under this Agreement. The parties shall agree, as part of the development of these mechanisms and procedures, as to which method, or combination of methods, of providing information will be sufficient for particular types or categories of information.

(r) *Responsible Officials for Information Sharing.* Until such time as modified by the parties, the responsible officials for information sharing under this Agreement are as follows:

(i) For the Secretary of Homeland Security, the Undersecretary for Information Analysis and Infrastructure Protection, or another individual designated by the Secretary to act in this capacity;

(ii) For the Attorney General, Executive Assistant Director for Counterterrorism and Counterintelligence; and

(iii) For the Director of Central Intelligence, the Associate Director of Central Intelligence for Homeland Security.

(s) *Provision of Covered Information to the DHS Directorate of Information Analysis and Infrastructure Protection.* Until further agreement by the parties, or their designees, all covered information provided, including information provided, under current procedures, to existing elements transferred to DHS, e.g., the United States Coast Guard and the U.S. Customs Service, shall also be separately provided to the Directorate of Information Analysis and Infrastructure Protection, including, if agreed by the Secretary, via the TTIC. The Undersecretary for Information Analysis and Infrastructure Protection, or another individual designated by the Secretary to act in this capacity, shall work with entities not within the Directorate to ensure effective coordination of information.

(t) *Classified Information.* The head of each covered entity shall put procedures in place to ensure that each individual recipient of classified information has, and maintains, appropriate security clearances, training, and need-to-know to receive classified information at the level at which the recipient will receive such information. Individuals shall be designated at each covered entity at several levels of seniority to receive classified information judged by the originating agency to be sufficiently sensitive to require limited distribution. In rare cases, the parties expect that extremely sensitive information may be provided only to the Secretary or, as appropriate, the head of another covered entity. The head of each covered entity also shall ensure that all mechanisms and procedures for receiving, storing, and handling classified information meet established legal and regulatory standards. The policies and procedures governing access to covered information under this Agreement, including such information that is classified, shall apply without regard to whether that information is made available in written, oral, or electronic form, or to the means or mechanism by which it is communicated to the recipient.

(u) *Thresholds.* In order to ensure that the Department is provided with all information necessary to carry out its responsibilities, but is not inundated with unmanageable volumes of information below thresholds reasonable to perform its mission, as soon as practicable, the Secretary shall advise the other parties, individually or collectively, as to establishing additional thresholds for information sharing, consistent with the DHS Legislation. For example, the Secretary may determine that low-level information concerning purely indigenous foreign terrorist groups with no apparent capability to mount operations against the United States is not relevant to DHS' mission. Such further agreement shall be consistent with the DHS Legislation and other relevant statutory authorities, Presidential Directives, the President's announced policies for protecting against terrorist threats to the homeland, and this Agreement. At any time following such initial agreement, the parties may agree to additional information sharing, or to more or less restrictive thresholds, as the volume of information involved and the needs of DHS become clearer, so long as such agreements are consistent with the DHS Legislation and this Agreement. Such agreements may be made by designees of the parties.

(v) *Privacy.* All information sharing pursuant to this Agreement shall be consistent with applicable privacy laws.

4. Coordination, Deconfliction, and Dispute Resolution.

(a) *Coordination and Deconfliction Policy.* Consistent with the President's direction that our highest priority is the protection of the American people from potentially devastating terrorist attacks, covered entities shall take all necessary measures to ensure that terrorist threats to our homeland are addressed cooperatively, efficiently, and with the understood overriding purpose of preventing, preempting, and disrupting those threats. To that end, the parties agree that no homeland security-related prevention, preemption, or disruption activity of any covered entity shall be presumed to be the best option in any given case, or otherwise deemed of higher precedence, importance, or

priority than any other such activity. The covered entities shall work together, to the greatest extent possible, to achieve, in each case, the maximum preventative, preemptive, and disruptive effect on potential threats, including coordinating simultaneous and complementary activities of multiple covered entities when appropriate. Because the failure to coordinate operational activities to preempt, prevent, and disrupt terrorist threats can create confusion, inefficiency and, in extreme cases, dangerous situations resulting from conflicting operational activities, the parties agree to coordinate operational activities to the greatest possible extent. Specifically, each party shall take all reasonable steps to ensure coordination and deconfliction of homeland security-related law enforcement, intelligence or national security-related activities of covered entities under that party's authority with such activities of other covered entities.

(b) *Analytic Conclusions and Supporting Information.* Terrorism and other homeland-security related analytic efforts of all covered entities must be informed by the most comprehensive, accurate, and timely information available, regardless of its nature and source, including, but not limited to, terrorism, WMD, vulnerabilities, and other pertinent information available to any covered entity. Analytic conclusions relating to terrorist or WMD threats to the homeland, or other issues within the responsibility of DHS, including information updating and amplifying previous conclusions, must be shared with all covered entities as soon as they are produced. Preemptive, preventative, and disruptive actions by all covered entities must be informed to the greatest extent possible by all available information and by all analytic conclusions, including competing conclusions, of all entities with relevant analytic responsibilities. At the same time, the Federal government must, to the greatest extent possible, speak with one voice to state and local officials, private industry, and the public, in order to prevent confusion, mixed signals, and, potentially, dangerous operational conflicts. In furtherance of these goals, the parties agree as follows:

(i) The parties shall ensure that covered entities disseminate their terrorism or other homeland security-related analytic products without delay to other covered entities that have related interests and responsibilities;

(ii) Except as otherwise provided in Sections 4(b)(iii) or (iv), no analytic conclusions, as defined in Section 2(a) of this Agreement, of any covered entity shall be disseminated to state, local, or private sector officials, or to the public, without the prior approval of the Secretary of Homeland Security, his designee, or in accordance with approval mechanisms, potentially including the TTIC or the JTTFs, established by the Secretary after the date of this Agreement.

(iii) Analytic conclusions may be provided directly to such officials or to the public where the head of a covered entity or his or her designee reasonably determines that exigent circumstances exist such that providing an analytic conclusion prior to required approval is necessary to prevent, preempt, or disrupt an imminent threat of death or serious bodily injury or significant damage to U.S. infrastructure or other interests. In the event an analytic conclusion is disseminated pursuant to the exigent circumstances exception in this paragraph,

the Secretary and other covered entities shall be notified immediately of the dissemination.

(iv) Analytic conclusions may be shared with federal, state, and local law enforcement officials without the prior approval of the Secretary of Homeland Security, provided, however, that it is the intention of the parties that DHS be provided with the earliest possible advance notice of the potential of such communications and, where possible, DHS will be included in the development of the communications through the DHS liaisons at FBI Headquarters. The Secretary of Homeland Security, or his designee (including a DHS representative to a JTTF if designated by the Secretary to do so), must approve further dissemination of such analytic conclusions to other non-law enforcement state and local officials or to the public.

(v) Nothing in this Agreement shall prevent covered entities from coordinating on analytic conclusions with, or seeking the views of, other Federal Government entities in evaluating terrorism or other homeland-security-related information.

(c) *Establishment of Mechanisms for Operational Coordination and Deconfliction.* As soon as practicable, the parties shall agree upon specific mechanisms, including technical, administrative, and, as appropriate, designation of focal points, to maximize the effectiveness of operational coordination and deconfliction. These will cover both overseas and domestic operations related to homeland security. Subsequent agreements for operational coordination and deconfliction may be reached upon the approval of the parties or their designees.

(d) *Information Sharing Dispute Resolution.* Consistent with the DHS Legislation and other relevant statutory authorities, Presidential Directives, the President's announced policies for protecting against terrorist threats to the homeland, the obligation to protect intelligence or sensitive law enforcement sources and methods from unauthorized disclosure, and with Section 3(a), and other relevant sections of this Agreement, issues concerning the application of the terms of this Agreement in any specific context with respect to whether particular covered information should be provided to the Department or to any other covered entity shall be handled under the following procedures:

(i) A holder of particular covered information at issue, whether within or outside the entity originating that information, shall refer the matter by the most expeditious means to the head of the entity originating the information (or that official's designee) for expeditious review.

(ii) The reviewing official shall, without exception, render a definitive decision on the request within 24 hours of receiving the referral and, in light of the access provisions in the DHS Legislation, shall resolve any doubt in favor of

providing the requested information.

(iii) If the originating agency's reviewing official declines to provide the covered information requested, that official shall, within the 24 hours allotted for response, provide the Department or other covered with --

- (A) the fact that the specific information is being withheld;
- (B) a succinct and specific statement of the reasons for the withholding; and
- (C) as much of the information requested as the head of the originating agency (or that official's designee) reasonably concludes can be provided given the President's announced policies for protecting against terrorist threats to the homeland, the DHS Legislation and other relevant statutory authorities, and relevant Presidential Directives.

(iv) If, at that point, a compromise is not reached expeditiously, the dispute will be resolved either by the Secretary, Attorney General, and DCI by mutual decision or through referral to the Assistant to the President for National Security Affairs and Assistant to the President for Homeland Security Affairs, or their designees, for resolution. Notwithstanding any other provision of this Agreement, the Attorney General, Secretary, or DCI, or their deputies may, whenever any of them deems it necessary or advisable (particularly when a fundamental matter of policy is implicated or time is of the essence), intervene to raise and resolve any issue of access to covered information by mutual decision or through the National Security Council and/or Homeland Security Council system.

(e) *NSPD-8*. Nothing in this Agreement in any way affects the responsibilities and authorities for coordination of United States counter-terrorism activities established in National Security Presidential Directive (NSPD) 8.

5. Protection of Intelligence and Sensitive Law Enforcement Sources and Methods.

The parties intend that all provisions of this Agreement be interpreted consistently with the DCI's statutory responsibility to protect intelligence sources and methods from unauthorized disclosure and with similar responsibilities of the Attorney General and the Secretary to protect sensitive law enforcement sources and methods, with the DHS Legislation and other relevant statutory authorities, Presidential Directives, the President's announced policies for protecting against terrorist threats to the homeland, and with Section 3(a), and other relevant provisions of this Agreement. Consistent with this agreed-upon interpretation:

- (a) The DCI shall carry out his responsibilities for the protection of intelligence sources and methods, and the Secretary and Attorney General shall carry out analogous responsibilities for sensitive law enforcement sources and methods, in a manner, and through mechanisms, that ensure that all covered information is made available promptly to the Department, and to other covered entities with a need-to-know and proper security clearances and handling procedures in place, subject only to such handling and use restrictions as are strictly and unavoidably necessary to protect

intelligence and sensitive law enforcement sources and methods from unauthorized disclosure.

(i) The DCI shall ensure that the substance of all covered information relevant to the responsibilities of all covered entities is provided to those entities in a form suited to their effective use of that information, consistent with the DCI's obligation to protect intelligence sources and methods from unauthorized disclosure and Section 3(a) of this Agreement. The Secretary and the Attorney General shall similarly ensure that the substance of covered information is provided in a suitable form.

(ii) The DCI shall ensure that dissemination of classified reporting based, wholly or in part, on covered information, is accompanied by dissemination of as much of that reporting and covered information as is possible at an unclassified (which may, when necessary, be marked "Sensitive-but-Unclassified" or "SBU") or reduced classification level, in order to ensure the broadest possible availability and use of covered information by those with a need-to-know that information (or information relating to that subject matter), based on a broad interpretation of the mission of the other covered entity. The Secretary and the Attorney General shall similarly ensure that dissemination is done in a manner that ensures the broadest possible availability.

(b) Information may be redacted or put into a tailored product to the extent consistent with Section 3(i) of this Agreement.

(c) Nothing in this section relieves any member of the Intelligence Community that originates covered information from its obligation to provide that information to DHS and other covered entities, as appropriate, in a form consistent with this Agreement, the DHS Legislation, and other relevant statutes and authorities regarding the protection of sources and methods.

6. "Sanitization" and Modification of Classification Levels for Further Sharing by DHS.

(a) Consistent with the President's announced policies, our national priorities, including this section, Section 3(a), and other relevant provisions of this Agreement, the DHS Legislation and other relevant statutes and Presidential Directives, covered entities that originate covered information that is classified shall retain the authority to determine whether that information, or any portions thereof, must remain classified in the interest of national security.

(i) Covered entities shall ensure that covered information that is classified or otherwise subject to restricted dissemination, but which reasonably appears likely to require onward passage to state, local, or private sector officials, the public, or other law enforcement officials for use in a criminal investigation, reaches DHS promptly with accompanying high-content "tear lines" suitable for onward passage at an unclassified level. Until this can be achieved



simultaneously to the transmission of covered information, the development of such tearlines shall not delay the provision of covered information.

(ii) The parties shall ensure, to the greatest extent possible, that covered entities utilize agreed-upon standardized formatting for preparation of tear-line material for passage to state, local, or private sector officials, including state and local law enforcement officials for use in a law enforcement investigation, or to the public, with the goal of providing necessary substantive information, but not enabling recipients to determine the originator, within the Federal government, of the information.

(b) DHS may, on its own initiative or at the request of a homeland security official to whom covered information is disseminated, ask that the originating agency declassify or reduce the classification level attached to that information in order to permit dissemination to additional officials who have a need-to-know the information, to promote ease of handling by those authorized to review it, to permit its incorporation into a document that is unclassified or classified at a lower level, or for other purposes consistent with the need promptly to provide homeland security officials with all relevant covered information that they have a need-to-know in the conduct of their official duties. Whenever it receives such a request, the originating agency shall respond to DHS, within 24 hours (or such longer period as is agreed to by all parties), unless compelling circumstances exist to require a longer response time. Such response will either –

(i) agree to declassify or reduce the classification level of the covered information in question as requested; or

(ii) provide an alternative formulation responsive to the requester's need for additional information sharing, but without declassifying or reducing the classification of the original document or covered information where that cannot be done consistent with assuring the national security.

(c) Where the need by DHS for further dissemination of classified information received from other covered entities, including through declassification or the preparation of unclassified tear-lines, is urgent because that information contains or may contain terrorist threat indications critical to the ability of homeland security officials to prevent, preempt, or disrupt a possible terrorist attack, that information may be passed directly to the entity or official that has a need-to-know that information, *provided that* the covered entity passing the information first notifies the originating agency and takes steps reasonable under the exigent circumstances to protect whatever classified information is not essential to initiating the urgent homeland security assurance measures that may be required.

(d) The parties agree to develop together, as soon as practicable, mechanisms and procedures, including through the use of detailees and assignees to the TTIC and JTTFs, as appropriate, to carry out the provisions of Section 6. The parties agree to work

together to ensure that the administrative, financial, and personnel burdens of this section are shared to the greatest extent possible among covered entities.

7. Detail or Assignment of Personnel. To facilitate the information sharing, coordination, and deconfliction policies covered in this Agreement, covered entities shall detail, and/or assign, to the greatest extent possible, including to the TTIC and/or JTTFs, personnel who have the authority either to make classification review and redaction decisions themselves, or, consistent with the time frames established in this Agreement, to refer those decisions to the appropriate officials at the originating agency for prompt action.

8. DHS Participation in Requirements Processes. As soon as practicable, the parties shall modify existing mechanisms and processes for prioritization of terrorism, WMD and other relevant foreign intelligence collection (including within the United States) and requirements processes to ensure that DHS has meaningful participation at each stage and level of each such mechanism or process, including through participation in the TTIC. The parties also shall work together to provide recommendations as to whether, and how, processes or mechanisms for purely "domestic" terrorism (e.g., concerning the capabilities, plans and intentions of exclusively domestic white supremacist or militia groups), and other relevant intelligence collection should be created or, alternatively, how to ensure meaningful participation by DHS in the prioritization for gathering such information. This section does not refer to operational activities.

9. Databases. The parties agree to establish procedures and mechanisms to provide DHS, and, as appropriate and practicable, other covered entities, with access to databases containing covered information. To this end, the parties shall establish a working group, within 30 days of the date of this Agreement. Developed procedures and mechanisms, including through the use of the TTIC and/or JTTFs, should be consistent with the DHS Legislation and other relevant statutory authorities, Presidential Directives, the President's announced policies for protecting against terrorist threats to the homeland, and the appropriate needs for access by DHS to appropriate databases, as well as with the protection of intelligence or sensitive law enforcement sources and methods, and with Section 3(a) and other provisions of this Agreement. Such procedures and mechanisms should facilitate, to the greatest possible extent: ease and speed of information exchange; differentiated access, to allow individuals with different levels of security clearance and need-to-know to have different levels of access to databases; and compatibility with other databases of covered entities.

10. Statement of Intent Concerning Information Technology. It is the intent of the parties to build and modernize all relevant databases and other information technology systems in order to maximize compatibility with other systems with which they must interact. Such procedures and mechanisms also must comply with existing statutory and Presidential Directives, including with regard to the protection of classified information and applicable privacy protections.

11. Handling and Storage. The parties shall ensure that covered entities within their jurisdiction observe the established handling and storage standards appropriate to the classification and access restrictions indicated on covered information they receive, use, and

disseminate, subject only to the provisions of this Agreement pertaining to exigent circumstances.

12. Information collected and shared by foreign governments. This Agreement contemplates a separate Memorandum of Understanding, consistent with this Agreement, being agreed to by the parties, that addresses concerns related to information collected and shared by foreign governments.

13. Implementation.

(a) Each of the parties shall implement their responsibilities under this Agreement as to the covered entities under their jurisdiction through such binding regulations, orders, directives, and guidance as necessary or prudent from time to time.

(b) Any authority or duty assigned herein to the Attorney General, the Secretary, or the DCI, may be delegated to one or more subordinate officials at the discretion of the official to whom the authority or duty is assigned, except as otherwise provided in this Agreement. Each such delegation shall be promptly communicated to all other parties.

14. No Private Rights Created. These procedures are not intended to and do not create any rights, privileges, or benefits, substantive or procedural, enforceable by any individual or organization against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

15. Counterpart Signatures. This Agreement may be signed in counterparts, each of which shall be considered to be an original.

s/s  
\_\_\_\_\_  
Attorney General

3-4-03  
Date

s/s  
\_\_\_\_\_  
Director of Central Intelligence

MAR 04 2003  
Date

s/s  
\_\_\_\_\_  
Secretary of Homeland Security

Feb. 28, 2003  
Date



## Executive Order 13388 of October 25, 2005

### Further Strengthening the Sharing of Terrorism Information to Protect Americans

By the authority vested in me as President by the Constitution and the laws of the United States of America, including [section 1016](#) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458), and in order to further strengthen the effective conduct of United States counterterrorism 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 State, local, and tribal governments, and between agencies and appropriate private sector entities; 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. Duties 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, 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 sections 102A(g) and (i) of the National Security Act of 1947, section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (including any policies, procedures, guidelines, rules, and standards issued pursuant thereto), sections 202 and 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; and
- (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.

Sec. 3. Preparing Terrorism Information for Maximum Distribution. To assist in expeditious and effective implementation by agencies of the policy set forth in section 1 of this order, the

common standards for the sharing of terrorism information established pursuant to section 3 of of August 27, 2004, shall be used, as appropriate, in carrying out of the Intelligence Reform and Terrorism Prevention Act of 2004.

Sec. 4. Requirements for Collection of Terrorism Information Inside the United States. To assist in expeditious and effective implementation by agencies of the policy set forth in section 1 of this order, the recommendations regarding the establishment of executive branch-wide collection and sharing requirements, procedures, and guidelines for terrorism information collected within the United States made pursuant to section 4 of Executive Order 13356 shall be used, as appropriate, in carrying out of the Intelligence Reform and Terrorism Prevention Act of 2004.

Sec. 5. Establishment and Functions of Information Sharing Council.

(a) Consistent with section 1016(g) of the Intelligence Reform and Terrorism Prevention Act of 2004, there is hereby established an Information Sharing Council (Council), chaired by the Program Manager to whom section 1016 of such Act refers, and composed exclusively of designees of: the Secretaries of State, the Treasury, Defense, Commerce, Energy, and Homeland Security; the Attorney General; the Director of National Intelligence; the Director of the Central Intelligence Agency; the Director of the Office of Management and Budget; the Director of the Federal Bureau of Investigation; the Director of the National Counterterrorism Center; and such other heads of departments or agencies as the Director of National Intelligence may designate.

(b) The mission of the Council is to (i) provide advice and information concerning 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; and (ii) perform the duties set forth in section 1016(g) of the Intelligence Reform and Terrorism Prevention Act of 2004.

(c) To assist in expeditious and effective implementation by agencies of the policy set forth in section 1 of this order, the plan for establishment of a proposed interoperable terrorism information sharing environment reported under section 5(c) of Executive Order 13356 shall be used, as appropriate, in carrying out of the Intelligence Reform and Terrorism Prevention Act of 2004.

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; and  
(b) the term "terrorism information" has the meaning set forth for such term in section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004.

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 Organization Act (42 U.S.C. 7131), section 103 of the National Security Act of 1947 (50 U.S.C. 403-3), 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;

(iii) shall be implemented consistent with the Department of Homeland Security, on "Strengthening Information Sharing, Access, and Integration Organizational, Management, and Policy Development Structures for Creating the Terrorism Information Sharing Environment;"

(iv) 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; and

(v) shall be implemented in a manner consistent with section 102A of the National Security Act of 1947.

(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.

Sec. 8. Amendments and Revocation.

- (a) Executive Order 13311 of July 29, 2003, is amended:
  - (i) by striking "Director of Central Intelligence" each place it appears and inserting in lieu thereof in each such place "Director of National Intelligence"; and
  - (ii) by striking "103(c)(7)" and inserting in lieu thereof "102A(i)(1)".
- (b) Executive Order 13311 of August 27, 2004, is hereby revoked.

[signed:] George W. Bush  
THE WHITE HOUSE,  
October 25, 2005.

**Department of Justice Protocol Regarding Terrorist Nominations**



**Office of the Deputy Attorney General**  
Washington, D. C. 20530  
October 3, 2008

**MEMORANDUM FOR HEADS OF DEPARTMENT COMPONENTS**

**From:** The Deputy Attorney General  
**Subject:** Department of Justice Protocol Regarding Terrorist Watchlist Nominations

The attached protocol reflects a new policy for the Department's internal process for nominating individuals for the Terrorist Screening Database (TSDb).

The TSDb consolidates the U.S. Government's terrorism screening and lookout databases into a single integrated identities database. The TSDb is also known as the "watchlist." This protocol is designed to ensure consistent and appropriate handling of watchlist information. The protocol responds to issues raised by the report of the Inspector General, dated March 14, 2008, entitled "Audit of the U.S. Department of Justice Terrorist Watchlist Nomination Processes." Specifically, that report recommended that the Department adopt a general policy for submission of watch list nominations. Implementation of the attached protocol will accomplish that task.

All components are directed to comply with this protocol effective immediately.

**DEPARTMENT OF JUSTICE PROTOCOL  
REGARDING TERRORIST WATCHLIST NOMINATIONS**

**A. Background**

1. On September 16, 2003, the President directed the Attorney General in Homeland Security Presidential Directive 6 (HSPD-6) to "establish an organization to consolidate the Government's approach to terrorism screening and provide for the appropriate and lawful use of Terrorist Information in screening processes." Terrorist Information was specifically defined to mean "individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism."

2. Concurrent with the signing of HSPD-6, the *Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism* (TSC MOU), was signed by the Secretaries of State and Homeland Security, the Attorney General and

the Director of Central Intelligence (DCI) (on behalf of the entire U.S. Intelligence Community). The TSC MOU established the Terrorist Screening Center (TSC) to consolidate the Government's approach to terrorism screening and provide for the appropriate and lawful use of Terrorist Information, a term clarified by the inclusion of Terrorist Identifiers in a subsequent agreement of the parties. Under HSPD-6, the TSC was to develop and maintain a database, to the extent permitted by law, containing the most thorough, accurate, and current information possible about known or suspected terrorists. HSPD-6 requires that its implementation be consistent with the Constitution and applicable laws, including those protecting the rights of all Americans. The TSC created the Terrorist Screening Database (TSDB) to meet these goals. The TSDB consolidates the U.S. Government's terrorism screening and lookout databases into a single integrated identities database. The TSDB is also known as the "watchlist."

3. The TSC MOU also incorporated all provisions of the *Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing*, dated March 4, 2003 (the "Information Sharing MOU").

4. In 2004, the Secretaries of State, Treasury, and Defense became signatories to the Information Sharing MOU by signing Addendum A to the TSC MOU. By doing so, they agreed that all provisions of the TSC MOU and the Information Sharing MOU apply to all entities that are or become a part of their respective Departments.

5. A second addendum (Addendum B), which supplements and incorporates by reference all provisions of the TSC MOU, superseded Addendum A and was finalized on January 18, 2007. The Directors of National Intelligence, NCTC, and the TSC joined as signatories in Addendum B. Under paragraph (3) (b) of Addendum B the Parties agreed, to the maximum extent permitted by law, to "provide to the NCTC on an ongoing basis all Terrorism Information (as defined in the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, Section 1016(a) (4) [as amended to include homeland security information and weapons of mass destruction information] in their possession, custody, or control). Paragraph 7 of Addendum B introduces the term Terrorist Identifiers to more clearly describe the type of terrorism information that NCTC (and the Federal Bureau of Investigation (FBI) for Purely Domestic Terrorism Information, as defined in the TSC MOU) receives from interagency partners and subsequently shares with TSC for inclusion in the TSDB.

6. Executive Order 13354 (August 27, 2004) created the National Counterterrorism Center (NCTC) to serve as the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism, excepting purely domestic counterterrorism information. That same provision, however, provides that NCTC may receive, retain, and disseminate information from any Federal, State, or local government, or other source necessary to fulfill its responsibilities, giving NCTC authority to receive, retain, and disseminate domestic terrorism information.



7. Section 1021 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) amended the National Security Act of 1947 to codify the creation of NCTC. Pursuant to IRTPA, NCTC serves "as the central and shared knowledge bank on known and suspected terrorists and international terror groups." NCTC's centralized knowledge bank is known as the Terrorist Identities Datamart Environment (TIDE). Section 1021(c) on Domestic Counterterrorism Intelligence states NCTC "may, consistent with applicable law, the direction of the President, and guidelines referred to in section 102A(b), receive intelligence pertaining exclusively to domestic counterterrorism from any Federal, State, or local government or other source necessary to fulfill its responsibilities and retain and disseminate such intelligence."

8. To enhance information sharing, the President issued Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans* (October 25, 2005), which requires the head of each agency that possesses or acquires terrorism information to promptly give access to that information to the head of each other agency that has counterterrorism functions.

9. Pursuant to paragraph (2) of HSPD-6, NCTC is mandated to "provide [TSC] with access to all appropriate information or intelligence in the [NCTC's] custody, possession, or control that TSC] requires to perform its functions."

10. TIDE serves as the single source for the TSDB, except for Purely Domestic Terrorism Information, which is provided directly to the TSC from the FBI via a formalized procedure. Purely Domestic Terrorism Information is defined in the TSC MOU as "i.e., information about U.S. persons that has been determined to be purely domestic terrorism information with no link to foreign intelligence, counterintelligence, or international terrorism."

11. TIDE contains the identifying and derogatory information on known or appropriately suspected international terrorists and the FBI's Automated Case Support system contains supporting information regarding purely domestic terrorists. The TSDB contains the identifiers exported from TIDE and the identifiers of domestic terrorists exported by the FBI. As a result, the TSDB contains the U.S. Government's comprehensive database of both international and domestic Terrorist Identifiers.

## **B. Nominating Components**

1. The Department of Justice contains a number of components that may acquire information regarding domestic or international terrorists. These components include the FBI, the TSC, the National Security Division, the Criminal Division, the Civil Rights Division, the Drug Enforcement Administration, the United States Marshals Service, the Bureau of Alcohol, Tobacco, Firearms, and Explosives, The Federal Bureau of Prisons, the Executive Office of the United States Attorneys, the United States Attorneys, and the United States National Central Bureau.

2. The policy of the Department of Justice is for all components to provide the FBI with all domestic or international Terrorism Information or Terrorist Identifiers so that the FBI can make appropriate nominations to the consolidated terrorist watchlist. With one exception relating to TSC's authority in exigent circumstances, only the FBI is authorized to nominate domestic or international terrorists for inclusion in the TSDB on behalf of the Department of Justice. The FBI has implemented policies governing the submission of such nominations, including procedures to follow when adding, modifying, or deleting a TSDB record. In making any proposed recommendation for watchlisting, each DOJ component should ensure that the underlying information is reasonably accurate, relevant and timely. In addition, the TSC has implemented its *Protocol Regarding Terrorist Nominations*. These policies must be followed regarding all nominations from the Department of Justice.

3. The TSC, which is administered by the FBI and reports to the Attorney General, is permitted to make entries into the TSDB when exigent circumstances exist. Such expedited nominations *must* be made in compliance with the FBI nomination policies and the TSC's *Protocol Regarding Terrorist Nominations*.

4. The Joint Terrorism Task Forces (JTTF) are a multi-agency effort led by the Department of Justice and the FBI to combine and leverage law enforcement and intelligence community resources to protect the United States from terrorist attack. JTTFs are comprised of highly trained, locally based, investigators, analysts, linguists, and other specialists from Federal, state, local, tribal, territorial law enforcement and intelligence community agencies. The National JTTF was established in July 2002 to serve as the coordinating mechanism for the JTTFs.

5. Department of Justice components, other than the FBI or the TSC, are not permitted to make direct nominations to the TSDB. A Department of Justice component should inform the appropriate JTTF through disseminated intelligence reports, electronic communication, or other method appropriate to the circumstances when it becomes aware of Terrorist Information, Terrorist Identifiers, or Purely Domestic Terrorism Information (collectively, Intelligence Information). The originating DOJ component should state whether it recommends watch listing the individual, the basis for that recommendation, and the investigative steps, if any, it has undertaken regarding the individual. If the JTTF determines that the information received from another component standing alone or in conjunction with other information known to the FBI meets the standards set forth in the Attorney General's Guidelines for opening a preliminary terrorism investigation or a full terrorism investigation and one has not been opened, the JTTF shall initiate an investigation and shall nominate case subjects for inclusion in TIDE and/or the TSDB in accordance with FBI policy, by forwarding all Intelligence Information, as appropriate, to the FBI's Terrorist Review and Examination Unit (TREX) using the FD-930 form and process.

6. The relevant JTTF will notify the Department of Justice component that Intelligence Information provided by that component has been used, in whole or in part, as the basis for a nomination to the TSDB or the creation of a record in TIDE. To the extent possible,

the relevant JITF will assign a representative from the nominating Department of Justice component to participate in the preliminary or full investigation that arises out of nominations from Department of Justice components. Once notified, the Department component will promptly provide FBI's TREX with additions, modifications, or deletions to a particular record as appropriate regarding that Intelligence Information via the component's JITF representative.

7. To prevent possible duplicate or partial reporting, the NCTC shall be informed that the FBI and the TSC are the sole TIDE and/or TSDB nominating agencies for the Department of Justice.

8. The provisions of this Protocol are not intended to prejudice, restrict, or interfere with any other agreement or arrangement of Department of Justice components, including arrangements related to law enforcement, exchange of information or counterterrorism efforts as appropriate.

All Department of Justice components should continue to share Intelligence Information as appropriate within the U.S. Intelligence Community.

## MEMORANDUM OF UNDERSTANDING ON TERRORIST WATCHLIST REDRESS PROCEDURES

The Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), the Terrorist Screening Center (TSC), the Department of Homeland Security (DHS), the Department of State (DOS), the Office of the Director of National Intelligence (ODNI), the National Counterterrorism Center (NCTC), the Central Intelligence Agency (CIA), the Department of Defense (DOD), and the Department of the Treasury (hereinafter referred to as the Parties);

Recognizing that the United States Government has developed a consolidated database of known and suspected terrorists that supports many different screening programs operated under distinct statutory and regulatory authorities;

Recognizing that agencies that contribute to, compile, distribute, and use the consolidated database must use best efforts to maintain current, accurate, and thorough information;

Recognizing that the implementation of the screening programs nonetheless may, at times, still cause inconvenience, delay, or other adverse experiences for individuals during the terrorism screening process;

Recognizing that complaints received regarding the terrorism screening process should be expeditiously reviewed and addressed with dignity and respect;

Recognizing that the experience of travelers and other individuals interacting with government screening personnel is potentially affected by factors outside the terrorism screening scope of this Memorandum of Understanding, including, for example, random screening, screening for involvement with illicit drugs or other illegal conduct, behavioral screening criteria, as well as the basic professionalism and courtesy of government screening personnel, and that attention to these factors must be promoted through other appropriate means within the respective jurisdictions of the Parties;

Recognizing that on January 17, 2006, the Departments of State and Homeland Security announced an initiative on "Secure Borders and Open Doors in the Information Age," otherwise known as the Rice-Chertoff Initiative, including the establishment of a redress process to address perceived problems in international and domestic traveler screening; and

Having consulted with the Privacy and Civil Liberties Oversight Board and the privacy and civil liberties officials of DHS, DOJ, and ODNI, in developing the procedures contained in this agreement;

Hereby enter into this Memorandum of Understanding (MOU).

## 1. BACKGROUND

Homeland Security Presidential Directive 6 (HSPD-6), "Integration and Use of Screening Information to Protect Against Terrorism," dated September 16, 2003, required the Attorney General to establish an organization to consolidate the Government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening processes. Also on September 16, 2003, and in support of HSPD-6, the Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism (HSPD-6 MOU) was signed by the Secretary of State, the Attorney General, the Secretary of Homeland Security, and the Director of Central Intelligence establishing TSC. On August 2, 2004, an addendum (Addendum A), which supplemented and incorporated by reference all provisions of the HSPD-6 MOU, was signed by the Secretary of the Treasury and the Secretary of Defense, in addition to the signatories of the HSPD-6 MOU. By their signatures on Addendum A, the Secretary of the Treasury and the Secretary of Defense also became signatories to the HSPD-6 MOU. In 2007, Addendum A was superseded by Addendum B, which added the Director of National Intelligence and the Director of the TSC as signatories.

## 2. PURPOSE, SCOPE, AND CONSTRUCTION

The purpose of this MOU is to set forth the mutual understanding of the Parties to establish and implement a coordinated redress process to respond to individual complaints about adverse experiences during terrorism screening that relate to the use of information contained in the government's consolidated database of known and suspected terrorists, known as the Terrorist Screening Database or TSDB. This MOU is intended to complement, and shall not be construed to conflict with, the Constitution, statutes, or regulations of the United States or any Party's legal authority to process screening-related complaints or appeals. To the extent that any provision of this MOU conflicts with any Party's legal authority for screening or to hear appeals, the conflicting provisions of this MOU shall not apply. This MOU does not apply to individual complaints, or parts thereof, that pertain to screening experiences that are unrelated to the use of information contained in the TSDB.

Any reference in this MOU to a Party or Parties shall also be understood to refer to any components of such Party or Parties to the extent that such components fall within the definition of screening agency or nominating/originating agency as set forth below, or that such components have been designated by the Party or Parties as having obligations arising from this MOU. Nothing in this MOU precludes any Party from conducting periodic reviews of individuals in the TSDB to determine whether an individual should remain in the TSDB, have their TSDB status modified, or be removed from the TSDB. Nothing in this MOU shall be construed to interfere with, limit, or impede any Party's ability to protect information that is classified pursuant to Executive Order 12958, as amended, or is otherwise protected by law from disclosure.

### 3. DEFINITIONS

As used in this MOU, these terms or phrases are defined as follows:

- A. Complaint or Redress Complaint: An individual's statement about an allegedly adverse experience or outcome during a terrorism screening process, which usually includes a request for assistance or a remedy.
- B. Derogatory Information: The information relied upon or generated by a nominating/originating agency to support the nomination of an individual to the TSDB.
- C. Known or Suspected Terrorist: As defined by HSPD-6, an individual known or appropriately suspected to be or to have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism. Pursuant to HSPD-6, the TSDB shall include identifying information about all known or suspected terrorists.
- D. Misidentified Person: An individual who has had an adverse experience or outcome during terrorism screening because the individual is a near match to a known or suspected terrorist in the TSDB. Misidentified persons are not actually listed in the TSDB but usually share an identical or very similar name and date of birth with a person in the TSDB, which causes them to be delayed or otherwise inconvenienced during screening.
- E. Nominating Agency: A Federal agency that has determined that an individual is a known or suspected terrorist and nominates that individual to the TSDB based on information that originated with that agency and/or a third agency.
- F. Originating Agency: A Federal agency that generates derogatory or identifying information about a known or suspected terrorist.
- G. Personally Identifiable Information: Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means including any other information, which is linked to such individual.
- H. Redress: The process whereby an individual may seek the help of a screening agency in addressing the cause of an adverse experience or outcome related to the use of TSDB data by filing a complaint with the screening agency. The screening agency or its designee, in cooperation with TSC and the nominating/originating agency, provides assistance by determining the cause of that adverse experience, verifying that all relevant information relied upon in the screening process is thorough, accurate, and current, and making any warranted corrections to pertinent records. The redress process as defined in this paragraph does not apply to complaints related to the visa application process.
- I. Screening Agency: Any agency that conducts terrorism screening. A screening agency acquires information for the purpose of determining whether an individual is a known or suspected terrorist in the TSDB, and evaluates and/or uses that information in order to take a particular governmental action with respect to an individual, such as requiring additional physical security screening at an airport security checkpoint, determining admissibility into the United States, or similar

governmental action. The DOS and DHS shall not be considered screening agencies with respect to the visa application process.

- J. Terrorism Screening: The evaluation of an individual to determine whether he or she is a known or suspected terrorist identified in the TSDB in order to take a particular governmental action with respect to an individual, such as requiring additional physical security screening at an airport security checkpoint, determining admissibility into the United States, or similar governmental action.
- K. Terrorist Screening Database or TSDB: The Federal government's consolidated database that contains identifying information about known or suspected terrorists. It is also commonly known as the consolidated terrorist watchlist. The TSDB is a sensitive but unclassified database and does not contain any derogatory information.
- L. TIDE: NCTC's Terrorist Identities Datamart Environment (TIDE), which is a classified database containing the derogatory information that supports the nominations of known or suspected international terrorists to the TSDB.

#### 4. RESPONSIBILITIES OF THE PARTIES

- A. Responsibilities of All Parties:
  - i. Designation of Responsible Official. Each Party will identify a senior official who will be responsible for ensuring the Party's full participation in the redress process and overall compliance with this MOU. A Party may also designate redress officials for components of that Party that perform screening or nominating/originating agency functions. The Parties agree to identify these officials and exchange the names of these officials no later than 30 calendar days after this MOU becomes effective and update the information as needed thereafter.
  - ii. Resources. Subject to the availability of funds, each Party will identify and commit appropriate staff and other resources to carry out responsibilities under this MOU. This includes identifying the office(s) responsible for carrying out the Party's responsibilities pertaining to the processing of individual redress complaints as set forth in this MOU. The Parties agree to exchange the names and contact information for the responsible offices no later than 30 calendar days after this MOU becomes effective, and update the information as needed thereafter.
  - iii. Information Sharing. Each Party will share all information relevant to the resolution of a complaint with other Parties to the extent necessary to carry out this MOU or to defend any judicial challenge to the resolution of a complaint, consistent with legal requirements and classification and handling controls. A Party may provide the relevant information in a summarized or substituted format to protect sensitive sources and methods.
  - iv. Protection of Personally Identifiable Information. Each Party will take appropriate action to protect personally identifiable information (PII) in its own record systems related to a redress matter against unauthorized access

- and to ensure that PII is handled in a way that provides security and accountability. When Parties transmit PII related to a redress matter via non-electronic or electronic means, such as email, facsimile, portable media or otherwise, the Parties will properly mark the data and/or communications/media/device to provide appropriate notice of the existence of PII and will ensure the means of transmission are secured by encryption or equivalent protections.
- v. Administrative Record. Each Party will be responsible for maintaining the administrative records necessary to document its participation in the redress process.
  - vi. Updating Agency Records. Each Party that maintains data related to the terrorist watchlist in its paper and/or electronic recordkeeping systems will update its records (i.e., correct, modify, or delete) expeditiously once notified of a change to an individual's watchlist status as the result of the disposition of a redress matter. This provision applies to data in government information systems (e.g., TIDE, Treasury Enforcement Communications System/Interagency Border Inspection System (TECS/IBIS), No-Fly List, Consular Lookout And Support System) used for watchlist creation or screening purposes. It is not intended to require the Parties to change records that reflect actions already taken based on watchlist status, unless and only to the extent that the record will have an unwarranted adverse impact on the individual seeking redress.
  - vii. Litigation. Subject to paragraph 4.A.iii above, each Party agrees to cooperate with DOJ to assist in defending any judicial challenge to the resolution of a redress complaint processed under this MOU or a determination by a screening agency that relied in whole or in part on records or information in the TSDB. This provision shall not be construed to limit DOS's discretion under section 222(f) of the Immigration and Nationality Act (INA), 8 U.S.C. § 1202(f), concerning the disclosure of visa records in litigation.
  - viii. Privacy Act Compliance. In carrying out this MOU, each Party is responsible for its own compliance with the Privacy Act of 1974, 5 U.S.C. §§ 552a *et seq.*, in the collection, maintenance, use, and dissemination of personally identifiable information. Within 30 calendar days after the effective date of this MOU, each Party agrees to review its applicable Privacy Act system of records notices and any relevant forms used to collect information from the public where such information may ultimately be used during the redress process. Each Party agrees to make appropriate changes to those documents, if necessary, including the publication of new or modified routine uses to permit the sharing of information to resolve redress matters and related litigation.
  - ix. Record Retention. Each Party agrees to retain its redress records for at least six years from the date of final agency disposition. Agencies may



- elect to establish a longer retention period to meet statutory, regulatory, or operational requirements.
- x. Requests for Disclosure of TSDB Data. Unless and until TSC advises the Parties of an alternate procedure, each Party agrees that it will contact TSC's legal counsel if it receives a request for information or records that it knows would reveal an individual's status (positive or negative) in the TSDB or would otherwise reveal the contents of TSDB data. TSC legal counsel will provide timely guidance on how to respond to these requests. This provision also pertains to requests for TSDB data resident in supported screening systems, such as the No-Fly List, TECS/IBIS, the National Crime Information Center's Violent Gang and Terrorist Organization File (VGTOTF), and the DOS's Consular Lookout and Support System (CLASS).
- B. Responsibilities of Screening Agencies:
- i. Designation of Responsibilities. Any Party that is a screening agency may designate another Party, with the other Party's consent if needed, to perform the responsibilities outlined in section 4.B. of this MOU. In addition, where a screening agency is a component of a Party, the Party may determine at its discretion that any responsibility of that screening agency may be performed in whole or in part by the Party.
- ii. Resources. Subject to the availability of funds, each screening agency will designate or create an office to carry out its operational responsibilities for redress. Where a Party has several components that perform terrorism screening, the responsible official for that Party (*see* Section 4.A.i above) will determine whether a single centralized office or separate offices in the appropriate components, or some combination of the two, will perform this function. Subject to the availability of funds, each screening agency will commit sufficient and appropriate staff and resources to that office or offices to ensure redress complaints are processed in a timely and efficient manner. The screening agencies agree to notify the other Parties of the identity of and contact information for the designated offices under this paragraph no later than 30 calendar days after this MOU becomes effective and update that information as needed.
- iii. Receipt and Initial Processing of Complaints. Each screening agency will have a procedure for receiving complaints from members of the public. If the screening agency receives a complaint from an individual who appears to be in the TSDB and the complaint relates to an adverse effect in the screening process arising out of his/her placement in the TSDB, the agency will forward a copy of the complaint and related information to TSC within a reasonable time. The screening agency will be responsible for verifying the identity of the complainant in accordance with the screening agency's applicable regulations and policies. When forwarding a complaint to TSC, the screening agency must provide: (1) all relevant correspondence from the individual, (2) copies of any relevant internal

- agency records, and (3) information identifying the complainant including, at a minimum, the complainant's full name, date of birth, and place of citizenship. After consultation with affected Parties, TSC may revise these requirements in the future as needed for expeditious processing of redress complaints. No amendment to the MOU would be required to effectuate such a change.
- iv. Follow-up with the Complainant. If requested by TSC, the screening agency will contact the complainant to request additional information to assist TSC or the nominating/originating agency in verifying the complainant's identity and processing the complaint. Nothing in this subsection precludes a screening agency from contacting the complainant in accordance with the screening agency's procedures or discretion.
- v. Response to the Complainant. Screening agencies are responsible for providing a written response to complaints they receive based on information provided by TSC and the nominating/originating agency. Because of the sensitivity of the TSDB and derogatory information, the content of any response to a complaint must be coordinated with TSC and the nominating/originating agency through TSC. Screening agencies may use standardized response letters that have been coordinated in advance by the screening agency, TSC, and DOJ.
- vi. Redress for Misidentified Persons. On January 17, 2006, DHS and DOS announced an initiative on "Secure Borders and Open Doors in the Information Age," otherwise known as the Rice-Chertoff Initiative, which includes the establishment of a redress process to address perceived problems in international and domestic traveler screening. The DHS Screening Coordination Office is leading the inter-agency effort to fulfill the goals of the Rice-Chertoff Initiative, which is intended to improve the redress process for persons who are misidentified during traveler screening processes, among other improvements.
- vii. Administrative Appeals. If the screening agency has established an administrative appeals process for redress determinations or other agency determinations in which the TSDB was used, the screening agency will notify TSC after receiving any such administrative appeal and work with TSC, as needed, to process the appeal, and coordinate the final agency response with TSC. The screening agency will provide all relevant paperwork to TSC (including a copy of the appeal letter and any information submitted by the individual on their own behalf). When the screening agency has the legal authority to make the final decision on the appeal, it will promptly notify TSC of that decision.
- viii. Litigation. When the screening agency becomes aware of litigation arising out of terrorism screening, the screening agency will notify TSC and DOJ as soon as possible after identifying the nexus to the TSDB. Notification should occur as soon as the Party learns of an individual's intent to sue or immediately after being served with legal process.

- C. Responsibilities of the Terrorist Screening Center:
- i. Receipt and Coordination of Complaints. TSC will receive complaints from screening agencies and research them to determine the nature and cause of the individual's adverse experience. TSC will track all complaints and will be responsible for facilitating any inter-agency coordination necessary to properly research the complaint and respond to the screening agency regarding the outcome (e.g., any corrections made or recommended).
  - ii. Review of Basis for Inclusion in the TSDB. In cases where the complainant is or appears to be in the TSDB, TSC will provide copies of the complaint letter and other relevant information to NCTC and/or the nominating/originating agency to assist in the resolution of the complaint. TSC will then work with NCTC and/or the nominating/originating agency, as appropriate, to determine whether the complainant's current status in the TSDB is appropriate based on the most current, accurate, and thorough information available. TSC may ask NCTC and/or the nominating/originating agency to provide updated information or analysis to assist in this determination as well as for a recommendation on addressing the complaint.
  - iii. Determination. After reviewing the available information and considering any recommendation from the nominating/originating agency, TSC will make a determination whether the record should remain in the TSDB, have its TSDB status modified, or be removed, unless the legal authority to make such a determination resides, in whole or in part, with another agency. In such cases, TSC will only prepare a recommendation for the decision-making agency and will implement any determination once made. TSC will take any necessary action to implement the determination, such as removing the record from the TSDB or modifying the record's status in the TSDB (e.g., downgrade from No-Fly to Selectee). Before taking action that is inconsistent with a recommendation of the nominating/originating agency, TSC will notify NCTC, which will convey that determination back to the nominating/originating agency, unless the nominating/originating agency is the FBI, in which case TSC will contact the FBI directly. The nominating/originating agency will then be responsible for addressing the conflict with TSC or the decision-making agency either directly or through NCTC. The Parties will then coordinate on an agreed-to resolution.
  - iv. Update of the TSDB. TSC will ensure that TSDB records are appropriately deleted or modified in accordance with a determination on a redress matter. TSC will also verify that such removals or modifications carry over to other screening systems that receive TSDB data (e.g., TECS/IBIS, No-Fly List).
  - v. Deconfliction. In the event of a multi-agency nomination where the nominating and/or originating agencies do not agree on what recommendation should be made on a specific redress matter, TSC will

request that the agencies consult with one another and share appropriate information about the watchlisted individual in an attempt to provide a joint recommendation to TSC. If the nominating/originating agencies cannot agree to a joint recommendation, TSC (or other agency with the legal authority to make the decision) will make the final determination considering the information provided by each agency.

- vi. Review Related to Misidentified Persons. If a complainant's adverse experience or outcome during terrorism screening is a result of being a near match ("misidentified") to a record in the TSDB, and that complaint is referred to TSC by the screening agency, TSC will review the record in the TSDB, as described in the paragraphs above, to ensure the TSDB record is valid and satisfies the criteria for inclusion in the TSDB and determine if additional information can be added to TIDE, the TSDB, or other agency systems to reduce the likelihood of a future misidentification. If the record does not meet the criteria, it will be removed from the TSDB.
- vii. Administrative Appeals. TSC will work with a screening agency to assist it in processing any administrative appeal of a redress determination or other determination in which the TSDB was used. When TSC receives notice of an appeal, TSC will notify NCTC and/or the nominating/originating agency as soon as possible. TSC will facilitate communications between the nominating/originating and screening agencies on the following issues: (1) determining what material may be releasable to the individual during appeal (if applicable), and (2) updating the analysis of any information that may have developed since the original determination and/or any information that was provided by the individual on his or her behalf during the appeals process itself. After reviewing the available information and considering any recommendation from the nominating/originating agency, TSC will make a determination whether the record should remain in the TSDB, have its TSDB status modified, or be removed, unless the legal authority to make such a determination resides, in whole or in part, with another agency. In such cases, TSC will only prepare a recommendation for the decision-making agency and will implement any determination once made.
- viii. Litigation. When TSC becomes aware of litigation arising out of terrorism screening, TSC will notify NCTC, the nominating/originating agency, and DOJ as soon as possible.

D. Responsibilities of the National Counterterrorism Center:

- i. Review, Coordination, and Research of Complaints. Upon receipt of a complaint from TSC, NCTC will review its holdings, notify the nominating/originating agency of the complaint, and provide the nominating/originating agency with a copy of the complaint for review.

NCTC will then request that the nominating/originating agency and, as appropriate, any other agency with relevant information, review their holdings and provide NCTC information relevant to the complaint. This may include updated information or analysis regarding the complainant's current status in the TSDB, derogatory information, identifying information that might be relevant to a misidentification, or other potentially relevant information or analysis (including that which tends to show that the individual is not a known or suspected terrorist, or which otherwise tends to cast doubt on the derogatory information). NCTC will also request that the nominating/originating agency provide its recommendation regarding resolution of the complaint. With the concurrence of the nominating/originating agency, NCTC will provide that agency's recommendation and any other relevant information to TSC. Should TSC or another agency disagree with the recommendation, NCTC will assist in the deconfliction process as set forth above. NCTC generally will not receive or process complaints or appeals for individuals nominated only by the FBI.

- ii. Review Related to Misidentified Persons. If a complainant's adverse experience or outcome during terrorism screening was the result of being a near match ("misidentified") to a record in the TSDB, and that complaint is referred to TSC by the screening agency, NCTC will work with TSC and the nominating/originating agency to ensure the TSDB record is valid and satisfies the criteria for inclusion in the TSDB, and determine if additional information can be added to TIDE, the TSDB, or other agency systems to reduce the likelihood of a future misidentification.
- iii. Update of TIDE. NCTC will promptly update TIDE records with any new derogatory or other relevant information (including that which tends to show that the individual is not a known or suspected terrorist, or which otherwise tends to cast doubt on the derogatory information) pertaining to individuals in the TSDB. NCTC will also modify TIDE in a timely fashion to reflect modifications to TSDB nominations resulting from a redress complaint and will make appropriate changes to a given TIDE record when it is necessary to trigger electronically conforming changes to the TSDB record.
- iv. Administrative Appeals. NCTC will work with TSC, as needed, to assist it in processing any administrative appeal of a redress determination or other determination in which the TSDB was used, including coordinating communication between TSC, the screening agency, and the relevant nominating/originating agency, as necessary. NCTC's primary role will be to coordinate administrative appeal requests by TSC with the appropriate nominating/originating agency in the Intelligence Community other than the FBI.

- L. Responsibilities of Nominating Originating Agencies:
- i. Review, Coordination, and Research of Complaints. Once notified of a redress complaint by TSC or NCTC, the nominating/originating agency will review the derogatory information that is the basis for including the complainant in the TSDB. In coordination with NCTC, when appropriate, the nominating/originating agency will evaluate whether the complainant continues to satisfy the criteria for inclusion in the TSDB, as well as any other relevant criteria, such as those for the No-Fly and Selectee Lists. The nominating/originating agency will determine whether updated information or analysis exists, including information from other agencies, and incorporate any such information in its response. The nominating/originating agency will also consider any information provided through the redress process by the individual, the screening agency, NCTC, or TSC. The nominating/originating agency shall take appropriate steps to modify, correct, or delete its holdings to reflect any changes made to TIDE as a result of the redress process, or that otherwise have been determined to be in error as a result of the redress process.
  - ii. Recommendation. The nominating/originating agency may make a recommendation to TSC as to the resolution of any complaint. Continued inclusion in the TSDB must be supported by derogatory information in TIDE. When the nominating/originating agency has additional derogatory or other relevant information that is not in TIDE, the nominating/originating agency will ensure that NCTC and TSC are notified, and will work with NCTC and TSC to ensure that such information is added to TIDE in a manner that provides meaningful information while protecting sources and methods. Every effort should be made, however, to share the derogatory information with TSC whenever possible.
  - iii. Deconfliction. In the event of a multi-agency nomination where the nominating and/or originating agencies do not agree on what recommendation should be made on a specific redress matter, the agencies will consult with one another at TSC's request and share appropriate information about the watchlisted individual in an attempt to provide a joint recommendation to TSC. If the nominating/originating agencies cannot agree to a joint recommendation, TSC will make the final determination considering all of the available information.
  - iv. Review Related to Misidentified Persons. If a complainant's adverse experience during terrorism screening was the result of being a near match ("misidentified") to a record in the TSDB, the nominating/originating agency of that record will work with TSC and NCTC, as appropriate, to ensure the TSDB record is valid and satisfies the criteria for inclusion in the TSDB, and if additional information can be added to TIDE, the TSDB, or other agency systems to reduce the likelihood of a future misidentification.

- v. Administrative Appeals. Each nominating/originating agency will work with TSC and NCTC, as needed, to assist them in processing an appeal of a redress determination or other determination in which the TSDB was used. The nominating/originating agency will be responsible for advising the screening agency on the releasability of any materials requested by an appellant during an appeal. An updated analysis of all relevant information will be coordinated between NCTC and the nominating/originating agency, and will be forwarded to TSC, which in turn will provide it to the screening agency. The analysis will consider any new information developed since the initial determination, as well as any information provided by the individual on his or her own behalf during the appeals process itself.
- F. Responsibilities of the Department of Justice:
- i. DOJ will coordinate with the relevant Parties during the defense of any judicial challenge to the resolution of a complaint processed under this MOU or a determination by a screening agency that relied in whole or in part on records or information in the TSDB.
  - ii. DOJ will consult with the Parties, as necessary, to provide continuing legal advice and support on matters related to watchlisting redress and this MOU.
- G. Visa Application Process; DOS and DHS Responsibilities at the Time of Visa Refusal:
- i. DOS and DHS will continue to comply with applicable visa procedures, which may include an at-post internal review by a supervisory consular officer or another appropriate official. While a consular officer's denial of a visa application may not be overruled, that determination is informed by an internal management review and, in appropriate cases, by input from an interagency review.
  - ii. If a visa application is refused, applicants are advised that they may re-apply for a visa. A subsequent application is considered as a new case. DOS agrees to continue to review the underlying data and facts in such subsequent applications. Whenever appropriate, DOS consults with TSC, NCTC, and other agencies regarding data that appears incomplete or inaccurate, or otherwise conflicts with information obtained in the visa application process.

## 5. SETTLEMENT OF DISPUTES

Except as set forth in paragraphs 4.C.v and 4.E.iii concerning the deconfliction of watchlist nominations, disagreements between the Parties arising under or related to this MOU will be resolved only by consultation between the Parties.

6. OTHER PROVISIONS

This MOU is not intended to conflict with either the Constitution or current federal statutes, regulations, or the directives of the Parties. If any term or provision of this MOU is inconsistent with such authority, then the term or provision shall be inapplicable to that Party and any other Party that is dependent upon the first Party's action to perform its responsibilities, but the remaining terms and conditions of this MOU shall continue to apply.

7. AMENDMENT

This MOU may be amended at any time by the mutual written consent of the Parties' authorized representatives. Modification within the scope of this MOU shall be made by the issuance of a fully executed addendum prior to any changes in responsibilities being performed.

8. TERMINATION

The terms of this MOU, as it may be amended, will remain in effect indefinitely. To terminate its participation in this MOU, a Party must give at least 30 days prior written notice. In the event of termination, each Party will continue with full participation up to the effective date of termination.

9. NO OBLIGATION OF FUNDS

This MOU does not constitute an obligation to expend funds by any Party. Unless otherwise agreed in writing, each Party shall bear any costs it incurs in relation to this MOU. Expenditures will be subject to federal budgetary processes and availability of funds pursuant to applicable laws and regulations. The Parties expressly acknowledge that this MOU in no way implies that Congress will appropriate funds for such expenditures.

10. NO PRIVATE RIGHTS

This MOU is an internal arrangement between the Parties and is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the Parties, their parent or component agencies, the United States, or the officers, employees, agents or other associated personnel thereof.

11. EFFECTIVE DATE

The terms of this MOU will become effective on the date on which it is signed by all Parties. The MOU may be signed in counterparts.

12. PERIODIC REVIEW

The Responsible Officials designated by the Parties pursuant to section 4.A.i will meet on an annual basis or at the request of any Party to discuss and review the implementation of this



MOU. Failure of the parties to conduct annual reviews will not result in the termination of activities provided for under this MOU.

13. POINTS OF CONTACT

Points of contact (POC's) for the Parties, identified below, are responsible for identifying the responsible officials and redress resources pursuant to sections 4.A.i and ii, and 4.B.ii and providing that information to the other POC's.

- A. The POC for the Department of Justice will be the Chief Privacy and Civil Liberties Officer.
- B. The POC for the Federal Bureau of Investigation will be the Section Chief of the National Threat Center Section, Counterterrorism Division.
- C. The POC for the Terrorist Screening Center will be the Privacy Officer.
- D. The POC for the National Counterterrorism Center will be the Chief of the Terrorist Identities Group.
- E. The POC for the Department of Homeland Security will be the Director of the Screening Coordination Office.
- F. The POC for the Department of State will be the Director of Information Management and Liaison Staff, Visa Office.
- G. The POC for the Office of the Director of National Intelligence will be the Civil Liberties Protection Officer.
- H. The POC for the Central Intelligence Agency will be the Chief of Policy and Community Action Staff (PCAS).
- I. The POC for the Department of Defense will be the Director, Joint Intelligence Task Force for Combating Terrorism, Defense Intelligence Agency.
- J. The POC for the Department of the Treasury will be the Assistant General Counsel (Enforcement and Intelligence).

The foregoing represents the understanding reached by the Parties.


**APPROVED BY:**

\_\_\_\_\_  
Condoleezza Rice  
Secretary of State

\_\_\_\_\_  
Date

\_\_\_\_\_  
Henry M. Paulson, Jr.  
Secretary of the Treasury

\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Alberto R. Gonzales  
Attorney General

3-6-07  
\_\_\_\_\_  
Date

\_\_\_\_\_  
Robert M. Gates  
Secretary of Defense

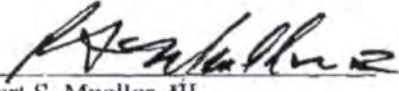
\_\_\_\_\_  
Date

\_\_\_\_\_  
Michael Chertoff  
Secretary of Homeland Security

\_\_\_\_\_  
Date

\_\_\_\_\_  
John D. Negroponte  
Director of National Intelligence

\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Robert S. Mueller, III  
Director, Federal Bureau of Investigation

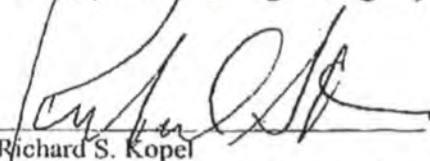
1/29/07  
Date

\_\_\_\_\_  
John Scott Redd  
Director, National Counterterrorism Center

\_\_\_\_\_  
Date

\_\_\_\_\_  
Gen. Michael V. Hayden  
Director, Central Intelligence Agency

\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Richard S. Kopel  
Acting Director, Terrorist Screening Center

1/19/07  
Date

The foregoing represents the understanding reached by the Parties.

**APPROVED BY:**

\_\_\_\_\_  
Condoleezza Rice  
Secretary of State

\_\_\_\_\_  
Date

\_\_\_\_\_  
Henry M. Paulson, Jr.  
Secretary of the Treasury

\_\_\_\_\_  
Date

\_\_\_\_\_  
Alberto R. Gonzales  
Attorney General

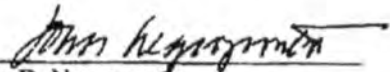
\_\_\_\_\_  
Date

\_\_\_\_\_  
Robert M. Gates  
Secretary of Defense

\_\_\_\_\_  
Date

\_\_\_\_\_  
Michael Chertoff  
Secretary of Homeland Security

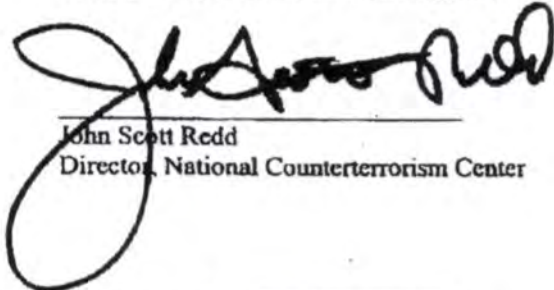
\_\_\_\_\_  
Date

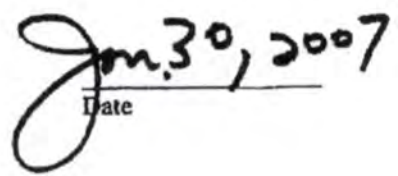
  
\_\_\_\_\_  
John D. Negroponte  
Director of National Intelligence

*February 5, 2007*  
\_\_\_\_\_  
Date

\_\_\_\_\_  
Robert S. Mueller, III  
Director, Federal Bureau of Investigation

\_\_\_\_\_  
Date

  
\_\_\_\_\_  
John Scott Redd  
Director, National Counterterrorism Center

  
\_\_\_\_\_  
Date

\_\_\_\_\_  
Gen. Michael V. Hayden  
Director, Central Intelligence Agency

\_\_\_\_\_  
Date

\_\_\_\_\_  
Richard S. Kopel  
Acting Director, Terrorist Screening Center

\_\_\_\_\_  
Date

The foregoing represents the understanding reached by the Parties

**APPROVED BY:**

\_\_\_\_\_  
Condoleezza Rice  
Secretary of State

\_\_\_\_\_  
Date

\_\_\_\_\_  
Henry M. Paulson, Jr.  
Secretary of the Treasury

\_\_\_\_\_  
Date

\_\_\_\_\_  
Alberto R. Gonzales  
Attorney General

\_\_\_\_\_  
Date

\_\_\_\_\_  
Robert M. Gates  
Secretary of Defense

\_\_\_\_\_  
Date

\_\_\_\_\_  
Michael Chertoff  
Secretary of Homeland Security

\_\_\_\_\_  
Date


3/1/07

\_\_\_\_\_  
John D. Negroponte  
Director of National Intelligence

\_\_\_\_\_  
Date

The foregoing represents the understanding reached by the Parties.

**APPROVED BY:**

  
\_\_\_\_\_  
Condoleezza Rice  
Secretary of State

05/17/2007  
Date

\_\_\_\_\_  
Henry M. Paulson, Jr.  
Secretary of the Treasury

\_\_\_\_\_  
Date

\_\_\_\_\_  
Alberto R. Gonzales  
Attorney General

\_\_\_\_\_  
Date

\_\_\_\_\_  
Robert M. Gates  
Secretary of Defense

\_\_\_\_\_  
Date

\_\_\_\_\_  
Michael Chertoff  
Secretary of Homeland Security

\_\_\_\_\_  
Date

\_\_\_\_\_  
John D. Negroponte  
Director of National Intelligence

\_\_\_\_\_  
Date

\_\_\_\_\_  
Robert S. Mueller, III  
Director, Federal Bureau of Investigation

\_\_\_\_\_  
Date

\_\_\_\_\_  
John Scott Redd  
Director, National Counterterrorism Center

\_\_\_\_\_  
Date

*Michael V. Hayden*  
\_\_\_\_\_  
Gen. Michael V. Hayden  
Director, Central Intelligence Agency

\_\_\_\_\_  
27 Apr '07  
Date

\_\_\_\_\_  
Richard S. Kopel  
Acting Director, Terrorist Screening Center

\_\_\_\_\_  
Date

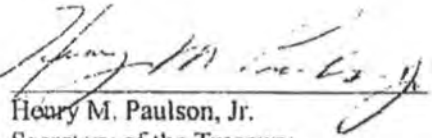


The foregoing represents the understanding reached by the Parties.

**APPROVED BY:**

\_\_\_\_\_  
Condoleezza Rice  
Secretary of State

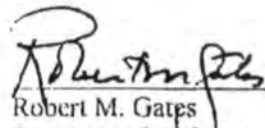
\_\_\_\_\_  
Date

  
Henry M. Paulson, Jr.  
Secretary of the Treasury

February 2, 2007  
Date

\_\_\_\_\_  
Alberto R. Gonzales  
Attorney General

\_\_\_\_\_  
Date

  
Robert M. Gates  
Secretary of Defense

9-19-07  
Date

\_\_\_\_\_  
Michael Chertoff  
Secretary of Homeland Security

\_\_\_\_\_  
Date

\_\_\_\_\_  
John D. Negroponte  
Director of National Intelligence

\_\_\_\_\_  
Date

January 7, 2010

MEMORANDUM FOR THE SECRETARY OF STATE  
 THE SECRETARY OF DEFENSE  
 THE ATTORNEY GENERAL  
 THE SECRETARY ENERGY  
 THE SECRETARY OF HOMELAND SECURITY  
 THE DIRECTOR OF NATIONAL INTELLIGENCE  
 THE DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY  
 THE DIRECTOR OF THE FEDERAL BUREAU OF  
 INVESTIGATION  
 THE DIRECTOR OF THE NATIONAL SECURITY AGENCY  
 THE DIRECTOR OF THE NATIONAL COUNTERTERRORISM  
 CENTER

SUBJECT: Attempted Terrorist Attack on December 25, 2009: Intelligence, Screening, and Watchlisting System Corrective Actions

After receiving the conclusions of the White House-led review of the U.S. watchlisting system and the performance of the intelligence, homeland security, and law enforcement communities as related to the attempt to bring down a Detroit-bound flight on December 25 by detonating an explosive device, and a Department of Homeland Security-led review on Aviation Screening, Technology and Procedures; I have concluded that immediate actions must be taken to enhance the security of the American people. These actions are necessary given inherent systemic weaknesses and human errors revealed by the review of events leading up to December 25<sup>th</sup>. They also are required to ensure that the standards, practices, and business processes that have been in place since the aftermath of 9/11 are appropriately robust to address the evolving terrorist threat facing our Nation in the coming years.

#### **Department of State**

- Review visa issuance and revocation criteria and processes, with special emphasis on counterterrorism concerns; determine how technology enhancements can facilitate and strengthen visa-related business processes.

#### **Department of Homeland Security**

- Aggressively pursue enhanced screening technology, protocols, and procedures, especially in regard to aviation and other transportation sectors, consistent with privacy

rights and civil liberties; strengthen international partnerships and coordination on aviation security issues.

- Develop recommendations on long-term law enforcement requirements for aviation security in coordination with the Department of Justice.

#### **Director of National Intelligence**

- Immediately reaffirm and clarify roles and responsibilities of the counterterrorism analytic components of the Intelligence Community in synchronizing, correlating, and analyzing all sources of intelligence related to terrorism.
- Accelerate information technology enhancements, to include knowledge discovery, database integration, cross-database searches, and the ability to correlate biographic information with terrorism-related intelligence.
- Take further steps to enhance the rigor and raise the standard of tradecraft of intelligence analysis, especially analysis designed to uncover and prevent terrorist plots.
- Ensure resources are properly aligned with issues highlighted in strategic warning analysis.

#### **The Central Intelligence Agency**

- Issue guidance aimed at ensuring the timely distribution of intelligence reports.
- Strengthen procedures related to how watchlisting information is entered, reviewed, searched, analyzed, and acted upon.

#### **Federal Bureau of Investigation/Terrorist Screening Center**

- Conduct a thorough review of Terrorist Screening Database holdings and ascertain current visa status of all "known and suspected terrorists," beginning with the No Fly list.
- Develop recommendations on whether adjustments are needed to the watchlisting Nominations Guidance, including biographic and derogatory criteria for inclusion in the Terrorist Identities Datamart Environment and Terrorist Screening Database, as well as the subset Selectee and No Fly lists.

#### **National Counterterrorism Center**

- Establish and resource appropriately a process to prioritize and to pursue thoroughly and exhaustively terrorism threat threads, to include the identification of appropriate follow-up action by the intelligence, law enforcement, and homeland security communities.

- Establish a dedicated capability responsible for enhancing record information on possible terrorists in the Terrorist Identities Datamart Environment for watchlisting purposes.

#### **National Security Agency**

- Develop and begin implementation of a training course to enhance analysts' awareness of watchlisting processes and procedures in partnership with National Counterterrorism Terrorist Center and the Terrorist Screening Center.

#### **National Security Staff**

- Initiate an interagency policy process to review the systemic failures leading to the attempted terror attack on December 25, 2009, in order to make needed policy adjustments and to clarify roles and responsibilities within the counterterrorism community.
- Initiate an interagency review of the watchlisting process, including business processes, procedures, and criteria for watchlisting, and the interoperability and sufficiency of supporting information technology systems.

I have designated my Assistant for Homeland Security and Counterterrorism John Brennan to be the responsible and accountable White House official to ensure rapid progress is made in all areas. A monthly status report on actions underway should be submitted to me through Mr. Brennan. In addition, I am directing Mr. Brennan to work with departments and agencies and the Office of Management and Budget on resource requirements that are necessary to address the shortcomings uncovered by our review. Finally, I will ask my Intelligence Advisory Board to look at broader analytic and intelligence issues associated with this incident, including how to meet the challenge associated with exploiting the ever-increasing volume of information available to the Intelligence Community. As we go forward, it is imperative that we work together to correct problems highlighted by this incident, focusing on concrete solutions. We are all responsible for the safety and security of the American people and must redouble our efforts to be effective in carrying out this solemn responsibility.



## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

Acronym	Description
Addendum B	Addendum B to the Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism, Signed by The Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of National Intelligence, the Director of the Central Intelligence Agency, the Director of the National Counterterrorism Center, the Director of the Terrorist Screening Center
A-File	Alien Registration File (DHS)
AIS	Automated Identification System
ALA	Airport Liaison Agents and Attaches (FBI)
API	Advanced Passenger Information
ATM	Automated Teller Machine
ATS	Automated Targeting System (DHS)
CBP	U.S. Customs and Border Protection (DHS)
CBRN	Chemical, Biological, Radiological, or Nuclear
CCD	Consular Consolidated Database (DOS)
CIA	Central Intelligence Agency
CJIS	Criminal Justice Information Services Division (FBI)
CLASS	Consular Lookout And Support System (DOS)
CTD	Counterterrorism Division (FBI)
DC	Deputies Committee
DCI	Director of Central Intelligence (now the DNI)
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency (DoD)
DoD	Department of Defense
DOJ	Department of Justice
DOMEX	Document and Media Exploitation
DOS	Department of State
DSR	Daily Summary Reports (TSC)
DTO	Designated Terrorist Organization
EFPs	Explosively Formed Projectiles/Penetrators
EMA	Encounter Management Application (TSC)
ERO	Enforcement and Removal Operations (DHS/ICE)
ESEL	Expanded Selectee List
ESTA	Electronic System for Travel Authorization
FBI	Federal Bureau of Investigation
FIN	Fingerprint Identification Number (DHS)
FISA	Foreign Intelligence Surveillance Act
FGI	Foreign Government Information
FTO	Foreign Terrorist Organization
FTTTF	Foreign Terrorist Tracking Task Force (FBI)
HAZMAT	Hazardous Materials
HSPD-11	Homeland Security Presidential Directive – 11, Comprehensive Terrorist-Related Screening Procedures

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

Acronym	Description
HSPD-24	Homeland Security Presidential Directive-24, Biometrics for Identification and Screening to Enhance National Security
HSPD-6	Homeland Security Presidential Directive-6, Integration and Use of Screening Information to Protect Against Terrorism
I&A	Office of Intelligence & Analysis (DHS)
IAFIS	Integrated Automatic Fingerprint Identification System (FBI/CJIS)
IAP	Immigration Advisory Program
ICE	U.S. Immigration and Customs Enforcement (DHS)
IED	Improvised Explosive Device
IIR	Intelligence Information Report
INA	Immigration and Nationality Act
Information Sharing MOU	Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing, dated March 4, 2003
IP	Internet Protocol
IPC	Interagency Policy Committee (IPC) is an interagency group led by the White House National Security Staff to establish Administration policies
IRTPA	Intelligence Reform and Prevention Act
ISA	The Information Sharing and Access Interagency Policy Committee (ISA IPC) is the White House led group that specifically addresses watchlisting policies for the U.S. Government
ISE	Information Sharing Environment
JTTF	Joint Terrorist Task Force
JWICS	Joint Worldwide Intelligence Communications System
KSTF	Known or Suspected Terrorist File (Federal Bureau of Investigation, National Crime Information Center, <i>formerly</i> Violent Gang and Terrorist Organization File ( <i>VGTOF</i> ))
LEGAT	Legal Attachés (FBI)
LEO	Law Enforcement Online
LPR	Lawful Permanent Resident
MOU	Memorandum of Understanding
NCIC	National Crime Information Center (FBI)
NCTC	National Counterterrorism Center
NDIU	Nominations and Data Integrity Unit (TSC)
NICS	National Instant Criminal Background Check System
NIPF	National Intelligence Priorities Framework
NIPF-CT	National Intelligence Priorities Framework - Counterterrorism
NIV	Non-Immigrant Visa
NMEC	National Media Exploitation Center
NORTHCOM	Northern Command (DoD)
NTC-C	National Targeting Center – Cargo (DHS/CBP)
NTC-P	National Targeting Center – Passenger (DHS/CBP)
NVMC	National Vessel Movement Center (DHS)

Appendix 10

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

Acronym	Description
OIA	Office of Intelligence and Analysis (DHS/TSA)
OTW	One Time Waiver
PIERS	Passport Information Electronic Records System
PNR	Passenger Name Records
POE	Port of Entry
RDD	Radioactive/Radiation Dispersal Device
Redress MOU	Memorandum of Understanding on Terrorist Watchlist Redress Procedures
SDGT	Specially Designated Global Terrorist
SDT	Specially Designated Terrorist
SIPRNET	Secret Internet Protocol Router Network
SME	Subject Matter Expert
SDNL	Specially Designated Nationals List
SRQ	Single Review Queue (TSC)
TACTICS	Tipoff Australia Counterterrorism information Control System
TBU	Threat-based expedited upgrade
TECS	<i>No longer an acronym.</i> Previously Treasury Enforcement Communications System.
TIDE	Terrorist Identities Datamart Environment
TIPOFF	<i>Not an acronym. Also seen as Tipoff.</i>
TREX	Terrorist Review and Examination Unit (TSC)
TRIP	Traveler Redress Inquiry Program (DHS)
TSA	Transportation Security Administration (DHS)
TSC	Terrorist Screening Center
<i>TSC MOU</i>	Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism
TSDB	Terrorist Screening Database
TSOC	Terrorist Screening Operations Center ( <i>formerly Terrorist Screening Tactical Operations Center (TSTOC)</i> )(TSC)
TSOU	Terrorist Screening Operations Unit (TSC)
TTIC	Terrorist Threat Integration Center (now NCTC)
TUSCAN	Tipoff United States Canada
TWIC	Transportation Worker Identification Credential (DHS/TSA)
U.S.	United States
U//FOUO	Unclassified, for official use only
UNSCR	United Nations Security Council Resolution
URL	Uniform Resource Locator
USAID	United States Agency for International Development
USCG	United States Coast Guard (DHS)
USCIS	U.S. Citizenship and Immigration Services (DHS)
USSS	United States Secret Service (DHS)
VIN	Vehicle Identification Number
WLS	Watchlist Service (DHS)

Appendix 10

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

UNCLASSIFIED//FOR OFFICIAL USE ONLY/ SENSITIVE SECURITY INFORMATION

## Summary of Changes and Updates from the 2010 Watchlisting Guidance



Appendix 11

(U//FOUO) The Watchlisting Guidance is a comprehensive document detailing the U.S. Government's terrorist watchlisting policies and procedures. It was originally developed to help standardize the watchlisting community's nomination and screening processes. Since approval of the Watchlisting Guidance in July of 2010, the guidance and its related appendices have undergone a thorough interagency review as a result of a May 2010 Deputy's Committee tasking to the White House National Security Staff Information Sharing and Access Interagency Policy Committee (IPC) that any significant issues or required changes be brought back to the Deputies for discussion. The Information Sharing and Access IPC identified a number of changes in Department and Agency watchlisting practices that had evolved since dissemination of the guidance in 2010. In order to reflect these changes, the 2013 Watchlisting Guidance was developed over a period of several months by an IPC under the auspices of the Presidential Policy Directive –One (PPD 1) process with representatives from the Departments of State, Treasury, Defense, Justice and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, the National Security Agency, the Defense Intelligence Agency, the National Counterterrorism Center, the Federal Bureau of Investigation, and the Terrorist Screening Center. The Deputies Committee adopted the recommendation of the IPC to approve the 2013 Watchlisting Guidance on March 12, 2013.

(U//FOUO) The 2013 Watchlisting Guidance has a new structure and is organized in a way that mirrors the watchlisting cycle. It is now a single document divided as follows into five chapters, with significant watchlisting foundational documents for reference, and a list of definitions, acronyms, and abbreviations:

- Chapter 1: Watchlisting Process and Procedures;
- Chapter 2: Minimum Identifying Criteria;
- Chapter 3: Minimum Substantive Derogatory Criteria;
- Chapter 4: No Fly, Selectee and Expanded Selectee Lists Implementation Guidance;
- Chapter 5: Encounter Management and Analysis;
- Appendix 1: Definitions;
- Appendix 2: Homeland Security Presidential Directive 6;
- Appendix 3: Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism (*TSC MOU*);
- Appendix 4: Addendum B to the *TSC MOU*;

UNCLASSIFIED//FOR OFFICIAL USE ONLY/ SENSITIVE SECURITY INFORMATION

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government Agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



UNCLASSIFIED//FOR OFFICIAL USE ONLY/ SENSITIVE SECURITY INFORMATION

- Appendix 5: Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing (*Information Sharing MOU*);
- Appendix 6: Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans;
- Appendix 7: Department of Justice Protocol on Terrorist Nominations;
- Appendix 8: Memorandum of Understanding on Terrorist Redress Procedures (*TSC Redress MOU*);
- Appendix 9: Presidential Memorandum Regarding 12/25/2009 Terrorist Attack;
- Appendix 10: Acronyms and Abbreviations;
- Appendix 11: Summary of Changes and Updates from the 2012 Watchlisting Guidance.

Appendix 11

(U//FOUO) The 2013 Watchlisting Guidance includes the following substantive policy changes and updates:

- New, amended, or clarified definitions are included for the terms “aggregator,” “derogatory information,” “encounter,” “enhancement,” “foreign fighters,” “fragmentary information,” “known terrorist,” “lone wolf,” “operationally capable,” “particularized derogatory information,” “reasonable suspicion,” “terrorism screening information,” “terrorism and/or terrorist activities,” and “U.S. Person” (Appendix 1);
- Nominators are instructed to send available information to the National Counterterrorism Center for consideration and additional review where reasonable minds could disagree on a record (Chapter 1);
- Nominating Departments and Agencies are instructed to prioritize the identification of new Known or Suspected Terrorists who meet the reasonable suspicion standard, along with the identifying and derogatory information most useful to the watchlisting and screening effort (Chapter 1);
- Nominating Agencies are to conduct periodic reviews of their nominations of U.S. Persons, at minimum on an annual basis (Chapter 1);
- Detailed instructions are described for handling U.S. Person information and ensuring that proper coordination processes are implemented (Chapters 1 and 3);
- The guidance regarding minimum identifying criteria has been revamped and exceptions clarified (Chapter 2);
- The guidance has been revised to provide Nominators with more flexibility regarding nominations of individuals based on fragmentary information (Chapter 2);
- The minimum substantive derogatory criteria guidance has been restructured to elaborate on instances of where particularized derogatory information is required to meet the reasonable suspicion standard, and when reasonable suspicion is established by other authority (Chapter 3);

UNCLASSIFIED//FOR OFFICIAL USE ONLY/ SENSITIVE SECURITY INFORMATION

UNCLASSIFIED//FOR OFFICIAL USE ONLY/ SENSITIVE SECURITY INFORMATION

- The minimum substantive derogatory criteria has been restructured to enable the watchlisting community to more clearly distinguish between watchlisting based on substantive derogatory criteria that meets the reasonable suspicion standard from watchlisting for purposes that support immigration and visa screening activities of the Department of Homeland Security and the Department of State (Chapter 3);
- Revised guidance is provided regarding the watchlisting of individuals based on information provided by a foreign government (Chapter 3);
- The guidance contains two additional categories of alien non-terrorists in the databases maintained by the National Counterterrorism Center and the Terrorist Screening Center to support immigration and visa screening activities of the Department of Homeland Security and the Department of State (*e.g.*, individuals who have a defined relationship with the Known or Suspected Terrorist, but whose involvement with the Known or Suspected Terrorist's activities is unknown (TIDE Category Code 50) and aliens for whom additional intelligence is required (TIDE Category Code 99)) (Chapter 3);
- The Implementing Guidelines regarding the No Fly and Selectee List criteria have been updated and clarified (*e.g.*, Guantanamo Bay detainees are now included on the No Fly List, as required by 49 U.S.C. Section 44903(j)(2)(C)(v)) (Chapter 4);
- Use of the One Time Waiver Policy is addressed to facilitate travel under controlled conditions of certain U.S. Citizen Known or Suspected Terrorists (Chapter 4);
- The guidance reflects the creation of the Expanded Selectee List, an export to the Transportation Security Administration of Known and Suspected Terrorist records within the Terrorist Screening Database that contain a full name and complete date of birth to support airline passenger screening (Chapter 4); and
- The guidance reflects the authority of the Terrorist Screening Center Director to make individual watchlist determinations (*i.e.*, placement on the No Fly, Selectee and Expanded Selectee Lists) during exigent circumstances (Chapter 4).

(U//FOUO) These changes to the Watchlisting Guidance are intended to make the watchlisting process more flexible, agile, and inclusive in order to respond to additional terrorism threats while providing the watchlisting community detailed guidance concerning the watchlisting policy of the U.S. Government.

(U//FOUO) The 2013 Watchlisting Guidance describes the U.S. Government's comprehensive watchlisting policies and process and includes Sensitive Security Information. Accordingly, Departments and Agencies who received copies of the 2013 Watchlisting Guidance are instructed to carefully control and share the guidance with only those individuals who are directly involved in the terrorist watchlisting and screening process.

UNCLASSIFIED//FOR OFFICIAL USE ONLY/ SENSITIVE SECURITY INFORMATION

UNCLASSIFIED//FOR OFFICIAL USE ONLY/ SENSITIVE SECURITY INFORMATION

(U) Nothing in the 2013 Watchlisting Guidance is intended to restrict the authority of any Department or Agency to act as provided by law, statute, or regulation, or to restrict any Agency from enforcing any laws within its authority or jurisdiction.

Appendix 11

UNCLASSIFIED//FOR OFFICIAL USE ONLY/ SENSITIVE SECURITY INFORMATION

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.