MEMORANDUM OF AGREEMENT BETWEEN THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE ON GUIDELINES FOR ACCESS, RETENTION, USE, AND DISSEMINATION BY THE NATIONAL COUNTERTERRORISM CENTER OF TERRORISM INFORMATION CONTAINED WITHIN DATASETS IDENTIFIED AS INCLUDING NON-TERRORISM INFORMATION AND INFORMATION PERTAINING EXCLUSIVELY TO DOMESTIC TERRORISM

I. Background

A. Pursuant to section 119(d) of the National Security Act of 1947, as amended, the National Counterterrorism Center (NCTC) shall "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 intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism." NCTC shall also "serve as the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support."

B. NCTC's analytic and integration efforts concerning terrorism and counterterrorism, as well as its role as the central and shared knowledge bank for known and suspected terrorists, at times require it to access and review datasets that are identified as including non-terrorism information and information pertaining exclusively to domestic terrorism in order to identify and obtain "terrorism information," as defined in section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004.[1] The President authorized such information sharing in Executive Order 13388, requiring that agencies place the "highest priority" on the "interchange of terrorism information" in order to "strengthen the effective conduct of United States counterterrorism activities and protect the territory, people, and interests of the United States of America." That Executive Order further requires that the "head of each agency that possesses or acquires terrorism information...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," consistent with law and statutory responsibilities. In the National Security Act of 1947, as amended, Congress, too, recognized that NCTC must have access to a broader range of information than it has primary authority to analyze and integrate if it is to achieve its missions. The Act thus provides that NCTC "may, consistent with applicable

[1] "The term 'terrorism information'—

(A) means all information whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—

(i) the existence, organization, capabilities, plans, intention, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;

(ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;

(iii) communications of or by such groups or individuals; or

(iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and

(B) includes weapons of mass destruction information." IRTPA, § 1016(a)(5).

law, the direction of the President, and the 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." National Security Act of 1947, as amended, section 119(e). Further, the Act envisions that NCTC, as part of the Office of the Director of National Intelligence (ODNI), *id.* at 119(a), would have the broadest possible access to national intelligence relevant to terrorism and counterterrorism. Section 102A(b) of the National Security Act of 1947, as amended, provides that "[u]nless otherwise directed by the President, the Director of National Intelligence shall have access to all national intelligence and intelligence related to the national security which is collected by any Federal department, agency, or other entity, except as otherwise provided by law or, as appropriate, under guidelines agreed upon by the Attorney General and the Director of National Intelligence."

C. This Memorandum of Agreement (MOA) establishes such guidelines between the Attorney General and the Director of National Intelligence as called for in section 102A of the National Security Act of 1947, as amended, to govern the access, retention, use, and dissemination by NCTC of terrorism information that is contained within datasets that are identified as including non-terrorism information and information pertaining exclusively to domestic terrorism. This MOA does not supersede the arrangements in place under the MOA for the Interagency Threat Assessment and Coordination Group (ITACG). See Homeland Security Act of 2002, as amended, section 210D, and the September 27, 2007 Memorandum of Agreement on the Establishment and Operation of the Interagency Threat Assessment and Coordination Group. The procedures for the ITACG MOA will be implemented consistent with this MOA. This MOA constitutes procedures pursuant to section 2.3 of Executive Order 12333 for NCTC's access to and acquisition of datasets explicitly covered by this MOA and govern, with respect to such activity, in lieu of the Attorney General-approved procedures pursuant to section 2.3 generally governing NCTC's or ODNI's access and acquisition activities. NCTC's retention, use, and dissemination of information contained in the datasets and all other NCTC activities remain subject to such generally applicable Attorney General-approved procedures, as well as additional applicable restrictions as set forth below. The terms and conditions of specific information acquisitions shall be determined by NCTC and the data provider and shall incorporate the guidelines agreed upon in this MOA.

II. References

A. National Security Act of 1947, as amended
B. Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, as amended
C. Homeland Security Act of 2002, as amended
D. Executive Order 12333 of December 4, 1981, as amended, "United States Intelligence Activities"
E. Executive Order 13388 of October 25, 2005, "Further Strengthening the Sharing of Terrorism Information to Protect Americans"
F. Homeland Security Presidential Directive (HSPD) 6 of September 16, 2003, "Integration and Use of Screening Information"
G. Director of Central Intelligence Directive (DCID) 6/3 of June 5, 1999, "Protecting Secure Compartmented Information within Information Systems," with appendices (or successor Intelligence Community Directives (ICD) and Policies)

H. December 4, 2006 Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment
I. March 4, 2003 Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing
J. September 27, 2007 Memorandum of Agreement on the Establishment and Operation of the Interagency Threat Assessment and Coordination Group
K. Central Intelligence Agency Headquarters Regulation 7-1 of December 23, 1987, "Law and Policy Governing the Conduct of Intelligence Activities"
L. National Counterterrorism Center Information Sharing Policy of February 27, 2006, "Rules of the Road" (NCTC Policy Document 11.2)
M. National Counterterrorism Center Role-Based Access Policy of November 9, 2006 (NCTC Policy Document 11.7)

III. Guidelines

A. Authority for and Scope of NCTC Data Access Acquisitions

1. NCTC information access, retention, use, and dissemination will be for authorized NCTC purposes. Pursuant to Executive Order 13388 and consistent with the National Security Act of 1947, as amended, and the March 4, 2003 Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing, NCTC shall be afforded prompt access to all Federal information and datasets that may constitute or contain terrorism information. NCTC may access datasets that may constitute or contain terrorism information, including those identified as containing non-terrorism information or information pertaining exclusively to domestic terrorism, to acquire, retain, and disseminate terrorism information pursuant to NCTC's statutory authorities consistent with these guidelines.

2. With respect to NCTC data access acquisitions covered by this MOA, NCTC will retain, use, and disseminate information on United States persons, as defined in Executive Order 12333, as amended, only if the information is reasonably believed to constitute terrorism information and only in accordance with the procedures set forth in sections III.B and III.C below, or for the purposes described in section III.A.3 below. Information is "reasonably believed to constitute terrorism information" if, based on knowledge and experience of counterterrorism analysts as well as the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the information is terrorism information.

3. These guidelines permit NCTC to acquire United States person information for the purpose of determining whether the information constitutes terrorism information and thus may be retained, used, and disseminated. Any such United States person information acquired must be promptly reviewed for such purpose. Information on United States persons that NCTC has erroneously acquired, for which the designation as terrorism information is subsequently discounted, or as to which a reasonable belief that it constitutes terrorism information cannot be

promptly established will not be retained, used, or disseminated. Such information will be promptly removed from NCTC's systems, unless such removal is otherwise prohibited by applicable law, regulation, policy, or court order. Information in NCTC systems found to contain errors will be promptly corrected to ensure information integrity and accuracy, and the data provider shall be notified of the error.

4. NCTC will acquire, retain, use, and disseminate information pursuant to the relevant standards of Executive Order 12333, as amended, and as consistent with the National Security Act of 1947, as amended, and other applicable provisions of law, including applicable privacy laws and laws and regulations governing the acquisition of information. NCTC users of acquired information will be subject at all times to NCTC's Role-Based Access and Information Sharing Policies, referenced above in section II, as well as additional audit and oversight authorities, as applicable. In implementing these guidelines, NCTC shall consult with the ODNI's Office of General Counsel (OGC) and the ODNI Civil Liberties Protection Officer (CLPO), as appropriate.

5. The Director, NCTC shall be the responsible official for ensuring that NCTC complies with the guidelines of this MOA. The CLPO shall be the responsible official for ensuring that NCTC, as part of the ODNI, complies with the Privacy Guidelines for the Information Sharing Environment, referenced above in section II.

B. General Procedures for NCTC Data Access Acquisitions

1. NCTC will work with the data provider to identify datasets that contain or may contain terrorism information, including those identified as containing non-terrorism information or information pertaining exclusively to domestic terrorism.

2. NCTC will coordinate its acquisitions of information with the data provider in advance to ensure that information is transmitted, stored, retained, accessed, used, and disseminated in a manner that protects privacy and civil liberties and information integrity and security and is in accordance with applicable laws and regulations. NCTC will work with the data provider to ensure acquired data is updated and verified throughout its retention and use by NCTC.

3. All NCTC personnel provided access to datasets under these guidelines will receive training in the use of the specific dataset, to ensure that NCTC personnel use the datasets only in accordance with authorized NCTC purposes. NCTC personnel will also receive ongoing training to ensure understanding of civil liberties and privacy expectations and requirements involved in the access to and use of datasets.

4. Use of acquired and retained information in disseminated NCTC products will be coordinated in advance with data providers to ensure that sensitive sources and methods, pending investigations, law enforcement equities, foreign government interests, privacy and civil liberties, and other considerations are appropriately protected. Information properly acquired and retained by NCTC may be used for all authorized NCTC purposes. This includes, but is not limited to: analytic and integration purposes, inclusion in finished analytic products and pieces,

enhancement of records contained within the Terrorist Identities Datamart Environment (TIDE), operational support, strategic operational planning, and appropriate dissemination to Intelligence Community, Federal, and other counterterrorism partners.

5. NCTC may make access to acquired information available to other parties only in accordance with the uses contemplated above and consistent with any other restrictions on the use of that information and after prior coordination with the data provider.

6. Information acquired pursuant to the tracks outlined below shall be deemed to remain under the control of the providing agency for purposes of the Freedom of Information Act, the Privacy Act, and any other legal proceeding, unless a different arrangement is agreed upon between NCTC and the providing agency.

C. Specific Procedures for NCTC Data Access Acquisitions

NCTC may acquire information contained within datasets in one or more of the three ways outlined below. NCTC will coordinate with the data providers to determine which information acquisition track provides the most effective means of ensuring NCTC access to terrorism information contained in the relevant datasets, consistent with the protection of privacy and civil liberties of United States persons. NCTC will work with data providers to ensure its access meets any additional necessary legal restrictions affecting provision of the specific data.

1. Track 1 Information Acquisition: Account-Based Access

a) NCTC personnel may be provided access to the datasets of other entities that may contain terrorism information either directly or through role-based accounts.

b) NCTC will access information in such datasets identified as containing non-terrorism information or information pertaining exclusively to domestic terrorism only to determine if the dataset contains terrorism information. NCTC may acquire, retain, use, and disseminate terrorism information consistent with all authorized NCTC purposes, as described above in sections III.A and III.B. If acquired information does not constitute terrorism information, NCTC will not retain, use, or disseminate the accessed information.

c) Consistent with section 119A of the National Security Act of 1947, as amended, and HSPD 6, the initial query term for NCTC access shall be a known or suspected terrorist identifier or other piece of terrorism information (hereinafter, "terrorism datapoints"). In order to follow up on positive query results, subsequent terrorism datapoints may be used to explore such known or suspected terrorist's network of contacts and support. NCTC is not otherwise permitted under these guidelines to query, use, or exploit such datasets (e.g., analysts may not "browse" through records in the dataset that do not match a query with terrorism datapoints, or conduct "pattern-based" queries or analyses without terrorism datapoints).

d) NCTC shall work with the dataset provider to ensure that terrorism datapoints and matching records from the dataset are provided, received, stored, and used in a secure

manner that appropriately protects intelligence sources and methods and related sensitivities, consistent with the requirements of DCID 6/3 or successor ICD.

2. Track 2 Information Acquisition: Search and Retention

a) NCTC may provide the owner of a dataset that may contain terrorism information with query terms–either singly or in batches–consisting of terrorism datapoints so that a search of the dataset may be run. Information from the dataset that is responsive to queries using NCTC-provided terrorism datapoints will be provided to NCTC. NCTC may acquire, retain, use, and disseminate this information consistent with all authorized NCTC purposes, as described above in sections III.A and III.B. Information not responsive to queries using terrorism datapoints will not be retained or accessible by NCTC.

b) By limiting NCTC search terms to terrorism datapoints, NCTC will receive only limited, preliminary access to information that may be either non-terrorism information or information pertaining exclusively to domestic terrorism. If later NCTC review of the received information reveals that specific information does not constitute terrorism information, NCTC will not retain, use, or disseminate that information.

c) NCTC shall work with the dataset provider to ensure that terrorism datapoints and responsive records from the dataset are provided, received, stored, and used in a secure manner that appropriately protects intelligence sources and methods and related sensitivities, consistent with the requirements of DCID 6/3 or successor ICD.

3. Track 3 Information Acquisition: NCTC Dataset Replication

a) NCTC may replicate portions or the entirety of a dataset when NCTC has determined, through its dataset identification process, that a dataset is likely to contain significant terrorism information, and that NCTC's authorized purposes cannot effectively be served through Tracks 1 or Track 2.

b) Dataset replication will be designed to exclude or remove United States person information that is not reasonably believed to be terrorism information through filtration and verification mechanisms occurring as part of and following the replication process. Datasets received in accordance with Track 3 may not be accessed or used by NCTC prior to replication, except as directly necessary to accomplish such replication, subject to procedures agreed upon with the dataset provider. Measures will be put in place to ensure that the dataset is received and stored in a manner to prevent unauthorized access and use prior to the completion of replication.

c) NCTC will promptly review the replicated data to ensure that United States person information that is not reasonably believed to be terrorism information has been removed. NCTC will not retain, use, or disseminate any such information. NCTC will work with data providers to ensure that every replication is tailored to meet these conditions and any additional necessary legal restrictions affecting provision of the specific data.

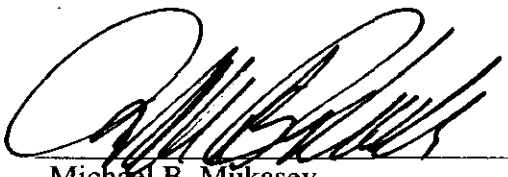
d) Once such replication process has occurred, NCTC may acquire, retain, use, and disseminate replicated information consistent with all authorized NCTC purposes, as described above in sections III.A and III.B, subject to the procedures in paragraph III.C.3.(f). Any data subsequently determined to be United States person information that is not reasonably believed to be terrorism information will be removed upon discovery.

e) By limiting NCTC replication to datasets that NCTC has determined contain significant terrorism information, NCTC will receive only limited access to information that may be either non-terrorism information or information pertaining exclusively to domestic terrorism outside the scope of NCTC's authorities.

f) NCTC shall work with the dataset provider to ensure that information for dataset replications are provided, received, stored, and used in a secure manner that appropriately protects intelligence sources and methods and related sensitivities, consistent with the requirements of DCID 6/3 or successor ICD.

IV. Period

This MOA shall be effective upon signature and shall remain in effect until revoked.



Michael B. Mukasey
Attorney General of the United States of America

11/4/08
Date

J. M. McConnell
Director of National Intelligence

1 OCT 08
Date