

**GUIDELINES FOR ACCESS, RETENTION, USE, AND DISSEMINATION
BY THE NATIONAL COUNTERTERRORISM CENTER AND OTHER AGENCIES
OF INFORMATION IN DATASETS CONTAINING
NON-TERRORISM INFORMATION**

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”; ensure that agencies “have access to and receive all-source intelligence support needed to execute their counterterrorism plans or perform independent, alternative analysis”; and “ensure that such agencies have access to and receive intelligence needed to accomplish their assigned activities.” Furthermore, any agency “authorized to conduct counterterrorism activities may request information” from NCTC “to assist it in its responsibilities.” *Id.* § 119(e)(2). Finally, the Director of National Intelligence (DNI) also has significant responsibilities for information sharing. He has “principal authority to ensure maximum availability of and access to intelligence information” within the Intelligence Community (IC). *Id.* § 102A(g)(1). When he establishes standards for facilitating access to and dissemination of information and intelligence, the DNI should give “the highest priority to detecting, preventing, preempting and disrupting terrorist threats and activities.” Executive Order 12333 § 1.3(b)(6)(A).

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 in order to identify and obtain “terrorism information,” as defined in section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, as amended.¹ “Non-

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, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;

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

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

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

(B) includes weapons of mass destruction information.” 6 U.S.C. § 485(a)(5).

UNCLASSIFIED

terrorism information” for purposes of these Guidelines includes information pertaining exclusively to domestic terrorism, as well as information maintained by other executive departments and agencies that has not been identified as “terrorism information” as defined by IRTPA. Included within those datasets identified as including non-terrorism information may be information concerning “United States persons,” as defined in Executive Order 12333 of December 4, 1981, as amended. The President authorized the sharing of terrorism information in Executive Order 13388 of October 25, 2005, and required 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 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 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 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, § 119(e). Further, the Act envisions that NCTC, as part of the Office of the Director of National Intelligence (ODNI), *id.* § 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. These Guidelines are established between the Attorney General and the Director of National Intelligence pursuant to section 102A(b) 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 maintained within other executive departments or agencies that are identified as including non-terrorism information. These Guidelines do not supersede the arrangements in place under the Memorandum of Agreement 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 (hereinafter the “ITACG MOA”). The procedures for the ITACG MOA will be implemented consistent with these Guidelines. These Guidelines also constitute procedures pursuant to section 2.3 of Executive Order 12333 for NCTC’s access to and acquisition of data concerning United States persons within the datasets explicitly covered by these Guidelines, and the retention and dissemination of such information from these datasets. The Attorney General-approved procedures pursuant to section 2.3 generally governing NCTC’s and ODNI’s access and acquisition activities (reference (o), below) are hereby superseded insofar as they apply to

UNCLASSIFIED

NCTC's retention, use, and dissemination of data and datasets governed by these Guidelines. NCTC's retention, use, and dissemination of information contained in the datasets governed by these Guidelines and all other NCTC activities remain subject to all other applicable laws and regulations. The terms and conditions of each specific information access or acquisition (hereinafter "Terms and Conditions") from another department or agency (hereinafter a "data provider") shall be developed in accordance with the provisions in section III.B.2 below, and shall be consistent with the Information Sharing Environment (ISE) guidelines issued pursuant to section 1016 of the IRTPA, to include the guidelines to protect privacy and civil liberties in the development and use of the information sharing environment.

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) Federal Agency Data Mining Reporting Act of 2007 (42 U.S.C. § 2000ee-3)
- e) 18 U.S.C. § 2332b(f) (Acts of terrorism transcending national boundaries—investigative authority)
- f) Executive Order 12333 of December 4, 1981, as amended, "United States Intelligence Activities"
- g) Executive Order 13388 of October 25, 2005, "Further Strengthening the Sharing of Terrorism Information to Protect Americans"
- h) Intelligence Community Directive (ICD) 501 of January 21, 2009, "Discovery and Dissemination or Retrieval of Information within the Intelligence Community"
- i) ICD 503 of September 15, 2008, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation"
- j) Director of Central Intelligence Directive (DCID) 6/3 of June 5, 1999, "Protecting Sensitive Compartmented Information within Information Systems," appendix E (or successor ICD and Policies)
- k) DCID 6/6 of July 11, 2001, "Security Controls on the Dissemination of Intelligence Information," (or successor ICD and Policies)
- l) 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
- m) March 4, 2003 Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing
- n) September 27, 2007 Memorandum of Agreement on the Establishment and Operation of the Interagency Threat Assessment and Coordination Group
- o) The Attorney General-approved procedures promulgated through Central Intelligence Agency Headquarters Regulation 7-1 of December 23, 1987, "Law and Policy Governing the Conduct of Intelligence Activities," as adopted by ODNI/NCTC, including any successor procedures (hereinafter "NCTC's EO 12333, § 2.3 Procedures")
- p) National Counterterrorism Center Information Sharing Policy of February 27, 2006, "Rules of the Road" (NCTC Policy Document 11.2) (or successor Policy)

UNCLASSIFIED

- q) National Counterterrorism Center Role-Based Access Policy of July 13, 2009 (NCTC Policy Document 11.7) (or successor Policy)
- r) ODNI Instruction 80.05, Implementation of Privacy Guidelines for Sharing Protected Information, September 2, 2009 (hereinafter "ODNI ISE Privacy Instruction")
- s) ODNI Instruction 80.02, Managing Breaches of Personally Identifiable Information, February 20, 2008.

III. Guidelines

A. Authority for and Scope of NCTC Data Access and Acquisitions

1. *Purpose and Authority.* NCTC's access to, and acquisition, retention, use, and dissemination of, information covered by these Guidelines 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 or acquire datasets that may constitute or contain terrorism information, including those identified as containing non-terrorism information, such as information pertaining exclusively to domestic terrorism and other information maintained by executive departments and agencies that has not been identified as terrorism information, in order to acquire, retain, and disseminate terrorism information pursuant to NCTC's statutory authorities consistent with these Guidelines.

2. *United States Person Information.* These Guidelines permit NCTC to access and acquire United States person information for the purpose of determining whether the information is reasonably believed to constitute terrorism information and thus may be permanently retained,² used, and disseminated. Any United States person information acquired must be reviewed for such purpose in accordance with the procedures below. Information is "reasonably believed to constitute terrorism information" if, based on the 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. *Erroneously Provided Information and Errors in Information.* Any United States person information that has been erroneously provided to NCTC will not be retained, used, or disseminated by NCTC. Such information will be promptly removed from NCTC's systems, unless such removal is otherwise prohibited by applicable law or court order or by regulation or policy approved by the Attorney General. 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 when feasible.

² For purposes of these Guidelines, "permanently retained" does not mean that the information is retained indefinitely, but rather that it is retained in accordance with NCTC's records retention policies.

UNCLASSIFIED

4. *Applicable Laws and Policies.*

a) NCTC will access, acquire, retain, use, and disseminate information, including United States person information, (i) pursuant to the relevant standards of Executive Order 12333, as amended; (ii) as consistent with the National Security Act of 1947, as amended; and (iii) as authorized by law or regulations, including applicable privacy laws. These Guidelines do not apply to information the retention, use, and dissemination of which is governed by court order or court-approved procedures.

b) NCTC shall not access, acquire, retain, use, or disseminate United States person information solely for the purpose of monitoring activities protected by the First Amendment or monitoring the lawful exercise of other rights secured by the Constitution or other laws of the United States. NCTC users of acquired information will be subject at all times to NCTC's Role-Based Access and Information Sharing Policies, to applicable ODNI Instructions, and to additional audit and oversight authorities and requirements, as applicable. In implementing these Guidelines, NCTC shall consult with the ODNI General Counsel and the ODNI Civil Liberties Protection Officer, as appropriate.

5. *Responsibility for Compliance.* The Director of NCTC, in consultation with the ODNI Office of General Counsel, shall be the responsible official for ensuring that NCTC complies with these Guidelines. The ODNI Civil Liberties Protection Officer shall oversee compliance with these Guidelines and compliance with other applicable laws, regulations, guidelines, and instructions as they relate to civil liberties and privacy.

B. General Procedures for NCTC Data Access and Acquisitions

1. *Identification of Datasets.* NCTC will coordinate with the data provider to identify datasets that are reasonably believed to contain terrorism information, including those identified as containing non-terrorism information.

2. *Establishing Terms and Conditions for Information Access.*

a) For access to or acquisition of specific datasets, the DNI, or the DNI's designee, shall collaborate with the data provider to identify any legal constraints, operational considerations, privacy or civil rights or civil liberties concerns and protections, or other issues, and to develop appropriate Terms and Conditions that will govern NCTC's access to or acquisition of datasets under these Guidelines. If either party believes that the Terms and Conditions do not adequately address the matters identified during that collaboration, that party may raise those concerns in accordance with the procedures in section III.B.2(d), below. These Guidelines do not alter any other obligations of a data provider to provide information to the DNI or NCTC. All Terms and Conditions shall incorporate these Attorney General-approved Guidelines, and shall ensure that information is transmitted, stored, retained, accessed, used, and disseminated in a manner that (i) protects privacy and civil liberties and information integrity and security, and (ii) is in accordance with applicable laws, regulations, guidelines and instructions (including the ODNI ISE Privacy Instruction). NCTC and the data provider will establish procedures to ensure the

UNCLASSIFIED

data provider notifies NCTC of any information the data provider believes, or subsequently determines to be, materially inaccurate or unreliable. NCTC will ensure mechanisms are in place at NCTC to correct or document the inaccuracy or unreliability of such information, and supplement incomplete information to the extent additional information becomes available. NCTC will work with the data provider to ensure that data acquired by NCTC under these Guidelines is updated and verified throughout its retention and use by NCTC, in accordance with the data quality, data notice, redress, and other applicable provisions of the ODNI ISE Privacy Instruction.

b) NCTC shall consult with the data provider to identify and put in place additional measures as necessary to honor obligations under applicable international agreements governing the information.

c) Any safeguards, procedures, or oversight mechanisms that go beyond those specified in these Guidelines shall be documented in the Terms and Conditions, and may include protections for sensitive sources and methods, pending investigations, law enforcement equities, foreign government interests, privacy and civil liberties, and similar considerations that apply to the use of the information. Any additional protective measures – such as the degree of advance coordination, if any, for dissemination of information obtained from a data provider – shall also be specified in the Terms and Conditions.

d) If the head of the department or agency providing the information or the DNI objects to providing data to NCTC, objects to the “track” under which NCTC intends to acquire the data, or objects to the Terms and Conditions developed after consultation (e.g., he or she believes that the Terms and Conditions do not adequately 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; do not adequately address operational equities; unnecessarily restrict sharing and use of the information; or are not in accordance with applicable laws, international agreements, and regulations), the head of the department or agency or the DNI may raise any concerns, in writing, with the other party. The head of the department or agency and the DNI shall attempt to resolve any such concern. Failing resolution, either party may refer a dispute concerning constitutional or other legal matters to the Attorney General and may seek the resolution of any other disputes through the National Security Council process. In connection with such disputes, the Attorney General or National Security Council may seek the advice of the Privacy and Civil Liberties Oversight Board.

3. *Training.* NCTC shall ensure that all NCTC employees, NCTC contractors, and detailees and assignees to NCTC from other agencies (hereinafter “NCTC personnel”) provided access to datasets under these Guidelines receive training in the use of each dataset to which they will have access to ensure that these personnel use the datasets only for authorized NCTC purposes and understand the baseline and enhanced safeguards, dissemination restrictions, and other privacy and civil liberties protections they must apply to each such dataset. These personnel will also receive ongoing training to ensure understanding of these Guidelines and civil liberties and privacy expectations and requirements involved in the access to and use of datasets governed by

UNCLASSIFIED

these Guidelines. The training required by this paragraph shall be in person whenever practicable and refreshed at least annually.

4. *Authorized Uses of Information.* Subject to any additional protections, requirements, or provisions in applicable Terms and Conditions, terrorism information, including terrorism information concerning United States persons, properly acquired and retained by NCTC may be used for all authorized NCTC purposes. These include, but are not limited to: analysis 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 elements, as well as federal and other counterterrorism partners. Specific provisions on use and dissemination are set forth in sections III.C and IV below, and any additional protections or provisions shall be specified in the Terms and Conditions.

5. *Information Access Requests.* For information acquired pursuant to the tracks outlined in section III.C below, it shall be the responsibility of the data provider to make determinations regarding the Freedom of Information Act and first-party access under the Privacy Act, and discovery or other requests for such information in any legal proceeding, unless a different arrangement is agreed upon between NCTC and the data provider and specified in the Terms and Conditions or is required by law. Information derived from an operational file exempted from search and review, publication, and disclosure under 5 U.S.C. § 552 in accordance with law shall remain under the control of the data provider and be handled as coordinated in advance with the data provider and specified in the Terms and Conditions for that information.

C. Specific Procedures for NCTC Data Access and Acquisitions

General. NCTC may acquire information contained within datasets governed by these Guidelines in one or more of the three ways outlined below. NCTC, in coordination with the data providers, will determine which information acquisition track, or tracks, 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, and any applicable legal requirements affecting provision of the specific data.

1. Track 1 Information Acquisition: Account-Based Access

a) *Type of Access.* NCTC personnel may be provided account-based access to the datasets of data providers that contain or may contain terrorism information (hereinafter "Track 1" access).

b) *Standard.* NCTC will access information in such datasets identified as containing non-terrorism information only to determine if the dataset contains terrorism information. NCTC may acquire, retain, use, and disseminate terrorism information for all authorized NCTC purposes, as described in these Guidelines. If the information acquired by NCTC is subsequently determined not to constitute terrorism information, NCTC will promptly purge any information the retention, use, or dissemination of which is not authorized by sections IV and V below.

UNCLASSIFIED

c) *Terrorism Datapoints.* Consistent with section 119 of the National Security Act of 1947, as amended, and section 1016(a)(5) of the IRTPA, as amended, the initial query term for NCTC Track 1 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 a known or suspected terrorist’s network of contacts and support. NCTC’s activities in Track 1 shall be designed to identify information that is reasonably believed to constitute terrorism information. NCTC is not otherwise permitted under these Guidelines to query, use, or exploit such datasets. For example, 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) *Protection of Sources and Methods.* NCTC shall work with the data 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 Appendix E of DCID 6/3 and ICD 503, or successor ICD.

2. Track 2 Information Acquisition: Search and Retention

a) *Type of Access.* NCTC may provide the owner of a dataset that contains or 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 (hereinafter “Track 2” access).

b) *Standard.* Information from the dataset that is responsive to queries using NCTC-provided terrorism datapoints will be given by the data provider to NCTC. NCTC may acquire, retain, use, and disseminate information acquired under Track 2 for all authorized NCTC purposes, as described in these Guidelines. NCTC’s activities in Track 2 shall be designed solely to identify information that is reasonably believed to be terrorism information. If the information given by a data provider to NCTC does not constitute terrorism information, NCTC will promptly purge any information whose retention, use, or dissemination is not authorized by sections IV and V below.

c) *Protection of Sources and Methods.* NCTC shall work with the data 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 and ICD 503, or successor ICD.

3. Track 3 Information Acquisition: NCTC Dataset Acquisition

a) *Type of Access.* NCTC may acquire and replicate portions or the entirety of a dataset when necessary to identify the information that constitutes terrorism information within the dataset (hereinafter “Track 3” access).

b) *Standard and Process.* Replication of data is appropriate when the Director of NCTC, or a designee who serves as Principal Deputy Director or as a Deputy Director (hereinafter “Designee”), determines in writing, after coordination with the data provider, that a dataset is

UNCLASSIFIED

likely to contain significant terrorism information and that NCTC's authorized purposes cannot effectively be served through Tracks 1 or 2. When making a determination, the Director or Designee also shall consider whether NCTC's authorized purposes can effectively be served by the replication of a portion of a dataset. Datasets received in accordance with Track 3 may not be accessed or used by NCTC prior to replication, except as directly necessary to make the determination above or to accomplish such replication, subject to procedures agreed upon with the data 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) Identification of United States Person Information and Temporary Retention Period. For all datasets received pursuant to Track 3, NCTC will use reasonable measures to identify and mark or tag United States person information contained within those datasets. Any United States person information acquired pursuant to Track 3 may be retained and continually assessed for a period of up to five years by NCTC to determine whether the United States person information is reasonably believed to constitute terrorism information (hereinafter "temporary retention period"). The Terms and Conditions shall establish the temporary retention period for continual assessment of such information. The temporary retention period specified in the Terms and Conditions may be up to five years unless a shorter period is required by law, including any statute, executive order, or regulation. In no event may NCTC retain the information for longer than is permitted by law. The temporary retention period shall commence when the data is made generally available for access and use following both the determination period discussed in section III.C.3(b) immediately above, and any necessary testing and formatting. United States person information that is reasonably believed to constitute terrorism information may be permanently retained and used for all authorized NCTC purposes, as described in these Guidelines.

d) Baseline Safeguards, Procedures, and Oversight Mechanisms. During the temporary retention period, the following baseline safeguards, procedures, and oversight mechanisms shall apply to all datasets acquired pursuant to Track 3 that have been determined to contain United States person information:

- (1) These datasets will be maintained in a secure, restricted-access repository.
- (2) Access to these datasets will be limited to those NCTC personnel who are acting under, and agree to abide by, NCTC's information sharing and use rules, including these Guidelines; who have the requisite security clearance and a need-to-know in the course of their official duties; and who have received the training required by section III.B.3.
- (3) Access to these datasets will be monitored, recorded, and audited. This includes tracking of logons and logoffs, file and object manipulation and changes, and queries executed, in accordance with audit and monitoring standards applicable to the Intelligence Community. Audit records will be protected against unauthorized access, modifications, and deletion, and will be retained for a sufficient period to enable verification of compliance with rules applicable to the data for which audit records apply.

UNCLASSIFIED

(4) NCTC's queries or other activities to assess information contained in datasets acquired pursuant to Track 3 shall be designed solely to identify information that is reasonably believed to constitute terrorism information. NCTC shall query the data in a way designed to minimize the review of information concerning United States persons that does not constitute terrorism information. To identify information reasonably believed to constitute terrorism information contained in Track 3 data, NCTC may conduct (i) queries that do not consist of, or do not consist exclusively of, terrorism data points, and (ii) pattern-based queries and analyses. To the extent that these activities constitute "data mining" as that term is defined in the Federal Agency Data Mining Reporting Act of 2007, the DNI shall report these activities as required by that Act.

(5) NCTC will conduct compliance reviews as described below in section VI.

e) *Enhanced Safeguards, Procedures, and Oversight Mechanisms.* In addition to the requirements of paragraph (d), at the time when NCTC acquires a new dataset or a new portion of a dataset, the Director of NCTC or Designee shall determine, in writing, whether enhanced safeguards, procedures, and oversight mechanisms are needed. In making such a determination, the Director of NCTC or Designee shall (i) consult with the ODNI General Counsel and the ODNI Civil Liberties Protection Officer, and (ii) consider the sensitivity of the data; the purpose for which the data was originally collected by the data provider; the types of queries to be conducted; the means by which the information was acquired; any request or recommendation from the data provider for enhanced safeguards, procedures, or oversight mechanisms; the terms of any applicable international agreement regarding the data; the potential harm or embarrassment to a United States person that could result from improper use or disclosure of the information; practical and technical issues associated with implementing any enhanced safeguards, procedures, or oversight mechanisms; and all other relevant considerations. If the Director of NCTC or Designee determines that enhanced safeguards, procedures, and oversight mechanisms are appropriate, the determination shall include a description of the specific enhanced safeguards, procedures, or oversight mechanisms that will govern the continued retention and assessment of the dataset. These enhanced safeguards, procedures, or oversight mechanisms may include the following:

- (1) Additional procedures for review, approval, and/or auditing of any access or searches;
- (2) Additional procedures to restrict searches, access, or dissemination, such as procedures limiting the number of personnel with access or authority to search, establishing a requirement for higher-level authorization or review before or after access or search, or requiring a legal review before or after United States person identities are unmasked or disseminated;
- (3) Additional use of privacy enhancing technologies or techniques, such as techniques that allow United States person information or other sensitive information to be "discovered" without providing the content of the information, until the appropriate standard is met;

UNCLASSIFIED

- (4) Additional access controls, including data segregation, attribute-based access, or other physical or logical access controls;
- (5) Additional, particularized training requirements for NCTC personnel given access or authority to search the dataset; and
- (6) More frequent or thorough reviews of retention policies and practices to address the privacy and civil liberties concerns raised by continued retention of the dataset.

Any enhanced safeguards, procedures, and oversight mechanisms must be included in the Terms and Conditions, or specified in writing and appended to the Terms and Conditions, and shall be kept on file as required by NCTC's record retention schedule.

f) *Removal of Information.* NCTC shall remove from NCTC's systems all identified information concerning United States persons that NCTC does not reasonably believe constitutes terrorism information within five years from the date the data is generally available for assessment by NCTC (or within the time period identified in the Terms and Conditions if the Terms and Conditions specify a shorter temporary retention period), unless such removal is otherwise prohibited by applicable law or court order or by regulation or policy approved by the Attorney General, or unless the information is retained for administrative purposes as authorized in section V below.

g) *Protection of Sources and Methods.* NCTC shall work with the data provider to ensure that information for dataset replications is 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 and ICD 503, or successor ICD.

IV. Dissemination

A. General Dissemination Requirements

1. *Definition.* For purposes of these Guidelines, dissemination means transmitting, communicating, sharing, passing, or providing access to information outside NCTC by any means, to include oral, electronic, or physical means.
2. *Terms and Conditions and Privacy Act.* All disseminations under these Guidelines must be: (i) compatible with any applicable Terms and Conditions or, if not compatible, the data provider must have otherwise consented to the dissemination; and (ii) permissible under the Privacy Act, 5 U.S.C. § 552a, if applicable.
3. *Dissemination to State, Local, or Tribal Authorities or Private-Sector Entities.* These Guidelines are not intended to alter or otherwise impact pre-existing information sharing relationships by federal agencies with state, local, or tribal authorities or private-sector entities, whether such relationships arise by law, Presidential Directive, MOU, or other formal agreement (including, but not limited to, those listed in section II above). To the extent that these

UNCLASSIFIED

Guidelines allow for dissemination to state, local, tribal, or private sector entities, such dissemination will continue to be made, consistent with section 119(f)(1)(E) of the National Security Act (50 U.S.C. § 404o(f)(1)(E)), in support of the Department of Justice (including the FBI) or the Department of Homeland Security responsibilities to disseminate terrorism information to these entities, and conducted under agreements with those Departments.

B. Dissemination of United States Person Information Acquired Under Tracks 1, 2, or 3

NCTC may disseminate United States person information properly acquired under Tracks 1, 2, or 3 if the General Dissemination Requirements are met, and if:

- (1) *Dissemination of Terrorism Information.* The United States person information reasonably appears to constitute terrorism information, or reasonably appears to be necessary to understand or assess terrorism information, and NCTC is disseminating the information to a federal, state, local, tribal, or foreign or international entity, or to any other appropriate entity that is reasonably believed to have a need to receive such information for the performance of a lawful function;
- (2) *Dissemination for Limited Purposes.* The United States person information is disseminated to other elements of the Intelligence Community or to a federal, state, local, tribal, or foreign or international entity, or to any other appropriate entity, for the limited purpose of assisting NCTC in determining whether the United States person information constitutes terrorism information. Any such recipients may only use the information for this limited purpose, and may not use the information for any other purpose or disseminate the information further without the prior approval of NCTC. Recipients of information under this paragraph must promptly provide the requested assistance to NCTC and promptly thereafter return the information to NCTC or destroy it unless NCTC authorizes continued retention after the specific information is determined by NCTC to meet the dissemination criteria in section IV.C.1 of these Guidelines. Recipients of information under this paragraph may not retain the information for purposes of continual assessment of whether it constitutes terrorism information unless such retention would be permitted by the dissemination criteria in section IV.C.1. Any access to or dissemination under this paragraph of any bulk dataset or significant portion of a dataset believed to contain United States person information must be: (i) approved by the Director of NCTC; and (ii) expressly allowed by the Terms and Conditions or otherwise expressly approved by the data provider. In addition, the recipient of any bulk dataset or significant portion of a dataset under this provision must agree in writing that it: (i) will not disseminate the information further without prior approval by NCTC; (ii) will use the data solely for the limited purpose specified in this provision; (iii) will promptly return the data to NCTC or destroy it after providing the required assistance to NCTC, unless NCTC authorizes continued retention of specific information after it is determined by NCTC to meet the dissemination criteria in section IV.C.1 of these Guidelines; (iv) will comply with any safeguards and procedures deemed appropriate by the ODNI General Counsel and ODNI Civil Liberties Protection Officer; and (v) will

UNCLASSIFIED

report to NCTC any significant data breach or failure to comply with the terms of its agreement. In deciding whether to approve dissemination under this paragraph of any bulk dataset or significant portion of a dataset, the Director of NCTC shall consider whether the limited purpose of this paragraph can be satisfied by allowing access to the data while it remains under NCTC's control and whether the recipient of the data has the capabilities necessary to comply with the requirements specified above;

- (3) *Dissemination Based on Consent.* The United States person whom the information concerns consents to the dissemination; or
- (4) *Dissemination of Publicly Available Information.* The United States person information is publicly available.

C. Dissemination of United States Person Information Acquired Under Track 3

1. *Standard (Non-bulk) Dissemination of Specific Information Acquired Under Track 3.* In addition to the provisions above for dissemination under all three tracks, NCTC may disseminate specific United States person information acquired under Track 3 that has been handled and subsequently identified in accordance with applicable Track 3 safeguards and procedures,³ if the General Dissemination Requirements are met, and if the United States person information:

- a) Reasonably appears to be foreign intelligence or counterintelligence, or information concerning foreign aspects of international narcotics activities, or reasonably appears to be necessary to understand or assess foreign intelligence, counterintelligence, or foreign aspects of international narcotics activities, and NCTC is disseminating the information to another federal, state, local, tribal, or foreign or international entity that is reasonably believed to have a need to receive such information for the performance of a lawful function, provided they agree to such further restrictions on dissemination as may be necessary;
- b) Reasonably appears to be evidence of a crime, and NCTC is disseminating the information to another federal, state, local, tribal, or foreign agency that is reasonably believed to have jurisdiction or responsibility for the investigation or prosecution to which the information relates and a need to receive such information for the performance of a lawful governmental function;
- c) Is disseminated to a Congressional Committee to perform its lawful oversight functions, after approval by the ODNI Office of General Counsel;
- d) Is disseminated to a federal, state, local, tribal, or foreign or international entity, or to an individual or entity not part of a government, and is reasonably believed to be necessary to: (i) protect the safety or security of persons, property, or organizations; or

³ This paragraph does not authorize NCTC to search for the additional categories of information, but rather allows NCTC to disseminate specific United States person information discovered while performing counterterrorism analysis and searches in accordance with these Guidelines and the applicable Terms and Conditions.

UNCLASSIFIED

- (ii) protect against or prevent a crime or a threat to the national security, provided they agree to such further restrictions on dissemination as may be necessary;
- e) Is disseminated to another federal, state, local, tribal, or foreign or international entity for the purpose of determining the suitability or credibility of persons who are reasonably believed to be potential sources or contacts, provided they agree to such further restrictions on dissemination as may be necessary;
- f) Is disseminated to another federal, state, local, tribal, or foreign or international entity for the purpose of protecting foreign intelligence or counterintelligence sources and methods from unauthorized disclosure;
- g) Is disseminated to other recipients, if the subject of the information provides prior consent in writing;
- h) Is otherwise required to be disseminated by statutes; treaties; executive orders; Presidential directives; National Security Council directives; Homeland Security Council directives; or Attorney General-approved policies, memoranda of understanding, or agreements; or
- i) Is disseminated to appropriate elements of the Intelligence Community for the purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it.

The identity of a United States person may be disseminated outside the Intelligence Community only if it is necessary or if it is reasonably believed that it may become necessary to understand and assess such information.

2. Bulk Dissemination of Information Acquired Under Track 3 to IC Elements. If the General Dissemination Requirements in section IV.A above are met, NCTC also may disseminate United States person information acquired under Track 3 to other IC elements under the following conditions:

- a) **General Requirements.** Any dissemination under these Guidelines of any bulk dataset or significant portion of a dataset believed to contain United States person information, which has not been assessed as constituting terrorism information, must be approved by the Director of NCTC and must be expressly allowed by the applicable Terms and Conditions for that dataset or otherwise expressly approved by the data provider. IC elements that receive or access bulk datasets or significant portions of a dataset under these Guidelines are not authorized to make further bulk disseminations of that information.
- b) **Bulk Dissemination in Support of Counterterrorism Missions:** The Director of NCTC shall only approve such dissemination to IC elements in support of a legally authorized counterterrorism mission if the receiving element head agrees in writing to abide by the

UNCLASSIFIED

provisions of the Appendix to these Guidelines and any enhanced safeguards, procedures, and oversight mechanisms identified in the Terms and Conditions for the particular dataset or otherwise required by the Director of NCTC.⁴ The agreement must specify, by name or position, the persons responsible for oversight and reporting, consistent with these Guidelines. The ODNI General Counsel and the ODNI Civil Liberties Protection Officer, in consultation with the Assistant Attorney General for National Security, shall verify that the receiving IC element has the capabilities and technology in place to accomplish the necessary oversight and compliance.

c) *Bulk Dissemination in Support of Other Intelligence Missions:* The Director of National Intelligence shall only approve such dissemination to IC elements in support of lawful intelligence missions other than counterterrorism missions if: such dissemination is expressly allowed by the applicable Terms and Conditions; the receiving element has Attorney General-approved procedures in place for the collection, retention, and dissemination of United States person information, as required by the opening paragraph of section 2.3 of Executive Order 12333; and the receiving element head agrees in writing to abide by safeguards, procedures, and oversight mechanisms substantially similar to the safeguards, procedures, and oversight mechanisms identified in the Appendix to these Guidelines, as well as any enhanced safeguards, procedures, and oversight mechanisms identified in the Terms and Conditions for the particular datasets or otherwise required by the Director of NCTC. In addition, the Director of National Intelligence may only approve bulk dissemination to IC elements in support of intelligence missions other than counterterrorism missions if the Director of National Intelligence, in consultation with the ODNI General Counsel, determines that the proposed dissemination is necessary to a lawful mission of the IC element and that the IC element's need for the information cannot be fulfilled through dissemination of specific information under the standard dissemination provisions of section IV.C.1; through dissemination of a smaller portion of the data proposed for dissemination; or by allowing access to the data while it remains within NCTC's control. The Director of National Intelligence will provide a copy of this determination to the Assistant Attorney General for National Security. The agreement must specify, by name or position, the persons responsible for oversight and reporting, consistent with these Guidelines. The ODNI General Counsel and the ODNI Civil Liberties Protection Officer shall verify that the receiving IC element has the capabilities and technology in place to accomplish the necessary oversight and compliance. Any such agreement must be approved by the Attorney General or his delegatee prior to allowing such dissemination, and the National Security Division of the Department of Justice may conduct an independent assessment of the element's oversight and compliance capabilities.

⁴ If an IC element with a counterterrorism mission requests changes to provisions in the Appendix to address agency-specific circumstances (e.g., technological capabilities), such changes may be adopted if expressly approved by the data provider and by the DNI and the Attorney General or their delegates, provided that any agency-specific Appendix shall retain safeguards, procedures, and oversight mechanisms substantially similar to those contained in the original Appendix.

D. Foreign Disseminations

For any dissemination of United States person information to a foreign or international entity, in addition to complying with the dissemination provisions of section IV, NCTC must find that: (i) the dissemination is consistent with the interests of the United States, including U.S. national security interests; (ii) the dissemination complies with DCID 6/6 or any successor ICD⁵; (iii) the foreign or international entity agrees not to disseminate the information further without approval by NCTC; and (iv) NCTC, in consultation with ODNI General Counsel, has considered the effect such dissemination may reasonably be expected to have on any identifiable United States person to determine whether any additional safeguards are needed.

E. Other Disseminations

If NCTC properly acquires any United States person information under Tracks 1 and 2 that would be authorized for dissemination pursuant to section IV.C.1 if it were acquired under Track 3, it shall consult with the data provider and advise the data provider of the existence of such information. The data provider may disseminate the information or authorize NCTC to do so.

V. Retention of Information for Administrative Purposes

To the extent consistent with law, United States person information acquired pursuant to these Guidelines may be retained if necessary to conduct the oversight, auditing, redress, or compliance activities required by these Guidelines, if required by law or court order to be retained, or if necessary to determine whether the requirements of these Guidelines or applicable laws are satisfied. Any information retained under this paragraph beyond the temporary retention period may not be used for purposes other than those specified in the preceding sentence and must be promptly removed from NCTC's systems once retention is no longer necessary or required for those purposes, except that NCTC may retain any oversight, audit, redress, or compliance records or reports in accordance with its records retention policies.

VI. Compliance

A. Periodic Compliance Reviews

Subject to oversight by the ODNI Civil Liberties Protection Officer, NCTC shall conduct periodic reviews to verify continued compliance with these Guidelines, including compliance with the Terms and Conditions, and with all baseline and enhanced safeguards, procedures, and oversight mechanisms. These reviews shall include spot checks, reviews of audit logs, and other appropriate measures.

⁵ ICD 403 is currently in draft. Once signed, any foreign dissemination would be required to comply with ICD 403 and any implementing ICPGs and IC Standards.

B. Periodic Reviews of the Need for Continued Assessment

NCTC, in coordination with the ODNI Civil Liberties Protection Officer, shall conduct periodic reviews of all datasets replicated under Track 3 to determine whether retention and continued assessment of the United States person information in those datasets remains appropriate. In conducting this review, consideration shall be given to the purpose for which the dataset was acquired, the success of that dataset in fulfilling legitimate counterterrorism purposes, whether those purposes can now be fulfilled through Track 1 or 2 access to the dataset, through the use of other datasets in NCTC's possession, or through other appropriate means, and privacy and civil liberties considerations applicable to the particular dataset. NCTC shall also conduct periodic reviews of the continued necessity and efficacy of bulk disseminations permitted under the Guidelines. NCTC shall report the results of these periodic reviews to the IC Inspector General.

C. NCTC's Computer Systems

In designing its computer systems, NCTC shall take reasonable steps to enhance its ability to monitor activity involving United States person information and other sensitive information, and to facilitate compliance with, and the auditing and reporting required by, these Guidelines.

D. Reporting

1. NCTC shall promptly report, in writing, to the Director of NCTC, the ODNI General Counsel, the ODNI Civil Liberties Protection Officer, the Department of Justice, and the IC Inspector General upon discovery of any significant failure to comply with: (i) these Guidelines; (ii) baseline or enhanced safeguards, procedures, or other oversight mechanisms; or (iii) any Terms and Conditions. For the purposes of these Guidelines, a "significant failure" is a failure that constitutes a violation of the Constitution or other law, including any executive order, and/or a failure that leads to unauthorized access, use, or dissemination of personally identifiable information about a United States person. NCTC shall report to any data provider whose information was affected by the noncompliance, in accordance with the Terms and Conditions for that data.

2. The Director of NCTC shall report annually in writing to the ODNI Civil Liberties Protection Officer on the measures that NCTC is taking to ensure that its access to, and retention, use, and dissemination of, United States person information is appropriate under these Guidelines and in compliance with the baseline and enhanced safeguards, procedures, and oversight mechanisms, and all applicable Terms and Conditions. The report shall include:

- (1) For datasets replicated under Track 3, the results of the review required in section VI.B above, regarding whether replication continues to be appropriate;
- (2) A general description of NCTC's compliance and audit processes;

UNCLASSIFIED

(3) A description of the audits, spot checks, and other reviews NCTC conducted during the previous year, and the results of those audits, spot checks, or other reviews, to include any shortcomings identified;

(4) A description of how NCTC ensures that it promptly purges United States person information that does not meet the standards for retention under these Guidelines;

(5) An assessment of United States person information disseminated by NCTC directly to foreign, international, state, local, tribal, or private sector entities or individuals; the restrictions, if any, that NCTC imposed on the entities' use or further dissemination of such information; and any known misuse of such information by a recipient, data breach, or significant failure by the recipient to comply with the terms of the certification required under section IV.B.2;

(6) A description of any approvals by the DNI or Director of NCTC, in accordance with sections IV.B.2 and IV.C.2 above, to provide access to or to disseminate bulk datasets or significant portions of a dataset;

(7) An assessment of whether there is a need for enhanced safeguards, procedures, or oversight regarding the handling of United States person information or other sensitive information, or whether any other reasonable measures that should be taken to improve the handling of information;

(8) A description of measures that NCTC has taken to comply with the requirements of section VI.C with respect to its data processing systems; and

(9) A description of any material changes or improvements NCTC implemented, or is considering implementing, to improve compliance with these Guidelines.

3. NCTC shall provide a copy of this report to the ODNI General Counsel and the IC Inspector General, and shall make the report available upon request to the Assistant Attorney General for National Security. NCTC shall also make available to the IC Inspector General any other reports or documentation necessary to ensure compliance with these Guidelines.

4. The reporting required by these Guidelines does not replace any other reporting required by statute, executive order, or regulation.

E. Privacy and Civil Liberties Oversight Board

Pursuant to section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004, the Privacy and Civil Liberties Oversight Board shall have access to all relevant NCTC records, reports, audits, reviews, documents, papers, recommendations, and other material that it deems relevant to its oversight of NCTC activities.

VII. Interpretation and Departures

A. NCTC shall refer all questions relating to the interpretation of these Guidelines to the ODNI Office of General Counsel. The ODNI General Counsel shall consult with the Assistant Attorney General for National Security regarding any novel or significant interpretations.

B. The ODNI General Counsel and the Assistant Attorney General for National Security must approve any departures from these Guidelines. If there is not time for such approval and a departure from these Guidelines is necessary because of the immediacy or gravity of a threat to the safety of persons or property or to the national security, the Director of NCTC or the Director's senior representative present may approve a departure from these Guidelines. The ODNI General Counsel shall be notified as soon thereafter as possible. The ODNI General Counsel shall provide prompt written notice of any such departures to the Assistant Attorney General for National Security. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States.

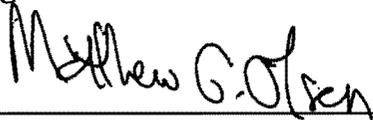
VIII. Status as Internal Guidance

These Guidelines are set forth solely for the purpose of internal NCTC and ODNI guidance. They are not intended to, and do not, create any rights, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies, or entities, its officers, employees, agents, or any other person, nor do they place any limitation on otherwise lawful investigative or litigation prerogatives of the United States.

IX. Revocations, Transitions, and Effective Date.

These Guidelines supersede and revoke the Memorandum of Agreement signed by the Director of National Intelligence and Attorney General on October 1, 2008 and November 4, 2008, respectively, along with any amendments to that Agreement. Terms and Conditions entered pursuant to that Memorandum of Agreement, or similar information sharing agreements to which NCTC is currently a party, remain in effect until revoked or until amended or replaced consistent with these Guidelines. As applied to NCTC, these Guidelines also supersede NCTC's EO 12333, § 2.3 Procedures with respect to the data and datasets covered by these Guidelines. These Guidelines shall be effective upon the approval of the Attorney General, the Director of National Intelligence, and the Director of NCTC.

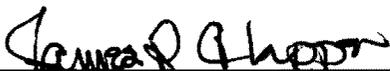
Signed



Matthew G. Olsen
Director, National Counterterrorism Center

MAR 21 2012

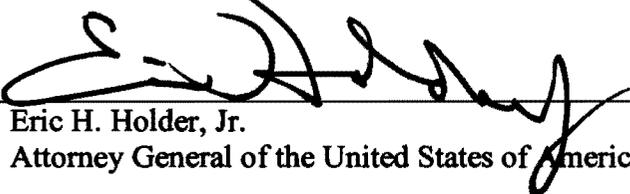
Date



James R. Clapper, Jr.
Director of National Intelligence

21 MAR 2012

Date



Eric H. Holder, Jr.
Attorney General of the United States of America

3 - 22 - 12

Date

UNCLASSIFIED

Appendix

Safeguards, Procedures, and Oversight Mechanisms for Bulk Dissemination of Information Acquired Under Track 3 to IC Elements

I. Purpose

This Appendix contains the safeguards, procedures, and oversight mechanisms that an Intelligence Community (IC) element head, or designee, must agree to, in writing, before NCTC may disseminate any bulk dataset or significant portion of a dataset (hereinafter referred to in this Appendix as “a dataset” or “data”) that includes United States Person information in accordance with section IV.C.2(b) of the NCTC Guidelines. NCTC may only disseminate datasets under this Appendix in support of the receiving IC element’s legally authorized counterterrorism mission.

II. Implementation

Prior to NCTC’s dissemination of any bulk dataset to an IC element, the element head must agree in writing to abide by the provisions of this Appendix, and any enhanced safeguards, procedures, and oversight mechanisms identified in the Terms and Conditions for the particular dataset or otherwise required by the Director of NCTC (hereinafter “written agreement”). All requirements shall be described, referenced, or appended to the written agreement, which the Director of NCTC shall develop in consultation with the ODNI General Counsel and Civil Liberties Protection Officer. If an IC element is provided access to NCTC’s systems in support of its legally authorized counterterrorism mission and NCTC will undertake any of the requirements in this Appendix on behalf of the IC element, the IC element head and the Director of NCTC shall specify in the written agreement the persons, by name or position, responsible for all training, oversight, and related compliance measures and reporting.

III. Definitions

For the purposes of this Appendix, the following definitions apply:

- A. Dissemination:** Dissemination means transmitting, communicating, sharing, passing, or providing access to information outside NCTC and/or the IC element by any means, to include oral, electronic, or physical means.
- B. IC Element:** The term “IC element” refers to the specific IC element that is provided data in accordance with section IV.C.2(b) of the NCTC Guidelines in support of the IC element’s legally authorized counterterrorism mission.
- C. Terrorism Information:** The term “terrorism information”—
 - (1) means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—

UNCLASSIFIED

UNCLASSIFIED

- (i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;
 - (ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;
 - (iii) communications of or by such groups or individuals; or
 - (iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and
- (2) includes weapons of mass destruction information. 6 U.S.C. § 485(a)(5).

D. United States Person. For an IC element receiving information under this Appendix, this term has the meaning given the term in that element's guidelines approved by the Attorney General under section 2.3 of Executive Order 12333. For an element without such Attorney General-approved guidelines, or whose guidelines do not contain such a definition, this term means 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. *See* Executive Order 12333 § 3.5(k).

IV. General Provisions

A. Authorized Purpose. The IC element may access and acquire United States person information in the dataset for the purpose of determining whether the information is reasonably believed to constitute terrorism information and thus may be permanently retained,¹ used, and disseminated. Any United States person information acquired must be reviewed for such purpose in accordance with the procedures in this Appendix, the applicable Terms and Conditions for that dataset, and any other measures specified in the written agreement. Information is "reasonably believed to constitute terrorism information" if, based on the 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.

B. Erroneously Provided Information and Errors in Information. Any United States person information that has been erroneously disseminated to the IC element will not be retained, used, or further disseminated by the IC element. Such information will be promptly removed from the IC element's systems, unless such removal is otherwise prohibited by applicable law or court order or by regulation or policy approved by the

¹ For purposes of this Appendix, "permanently retained" does not mean that the information is retained indefinitely, but rather that it is retained in accordance with the IC element's records retention policies.

UNCLASSIFIED

Attorney General. Information in the IC element's systems found to contain errors will be promptly corrected to ensure information integrity and accuracy, and NCTC shall be notified of the error promptly.

C. Removal of Information. The IC element shall remove from the IC element's systems all identified information concerning United States persons that the IC element does not reasonably believe constitutes terrorism information within five years from the date the data is generally available for assessment by NCTC (or within the time period identified in the written agreement if it specifies a shorter temporary retention period), unless such removal is otherwise prohibited by applicable law or court order or by regulation or policy approved by the Attorney General, or unless the information is retained for administrative purposes as authorized in section VII below.

D. Training. The IC element shall ensure that all employees and contractors of the IC element and detailees and assignees to the IC element from other agencies (hereinafter "IC element personnel") provided access to the data under this Appendix will receive training in the use of each dataset to which they will have access to ensure that they use the data only for the IC element's authorized counterterrorism purposes and in accordance with this Appendix and other applicable requirements. The training shall also ensure that they understand the baseline and enhanced safeguards, dissemination restrictions, and other privacy and civil liberties protections they must apply to each dataset. This training shall be in person, whenever practical, and refreshed at least annually. IC element personnel provided access to data under this Appendix will also receive ongoing training to ensure understanding of this Appendix and other applicable agreements and the civil liberties and privacy expectations and requirements involved in the access to and use of the data.

E. Authorized Uses of Information and Time Periods. For all datasets or data received pursuant to this Appendix, the IC element will use reasonable measures to identify and mark or tag United States person information contained within those datasets (to the extent not already done so by the data provider and NCTC). Any United States person information accessed or acquired in accordance with this Appendix may be continually assessed for up to five years by IC element personnel to determine whether the United States person information is reasonably believed to constitute terrorism information unless a shorter temporary retention period is specified in the written agreement with NCTC. The written agreement signed by the IC element head or designee shall specify the applicable temporary retention period for the dataset or data as required by the Terms and Conditions or otherwise required by the Director of NCTC. The temporary retention period shall commence when the data is made generally available for access and use by NCTC; the period is not restarted at the time of dissemination to or access by the IC element. United States person information that is reasonably believed to constitute terrorism information may be permanently retained and used for all authorized IC element purposes. These include, but are not limited to: analysis and integration purposes, inclusion in finished analytic products and pieces,

UNCLASSIFIED

enhancement of records contained within the Terrorist Identities Datamart Environment (TIDE), operational support and planning, and appropriate dissemination to Intelligence Community elements, as well as federal and other counterterrorism partners. Specific provisions on use and dissemination are set forth below. Any additional protections or provisions required by the Terms and Conditions for that dataset or otherwise required by the Director of NCTC must be included in the written agreement signed by the IC element head or designee.

F. Applicable Laws and Policies. The IC element shall access, acquire, retain, use, and disseminate information, including United States person information, (i) pursuant to the relevant standards of Executive Order 12333, as amended; (ii) as consistent with the National Security Act of 1947, as amended; and (iii) as authorized by law or regulations, including applicable privacy laws. This Appendix does not apply to information whose retention, use, and dissemination is governed by court order or court-approved procedures. If the IC element has Attorney General-approved procedures pursuant to section 2.3 of Executive Order 12333, those are hereby superseded as applied to the collection, retention, and dissemination of United States person information in data and datasets governed by this Appendix, except as otherwise specifically provided herein.

G. Limitation. The IC element shall not access, acquire, retain, use, or disseminate United States person information solely for the purpose of monitoring activities protected by the First Amendment or monitoring the lawful exercise of other rights secured by the Constitution or other laws of the United States. IC element personnel who access NCTC's databases will be subject at all times to NCTC's Role-Based Access and Information Sharing Policies, and to additional audit and oversight requirements, as applicable and as specified in the written agreement signed by the IC element head or designee. IC elements may be required to adopt or apply similar role-based access and information sharing policies prior to receiving and storing data from NCTC; any such requirements will be specified in the written agreement signed by the IC element head or designee.

H. Information Access Requests. For information governed by this Appendix, it shall be the responsibility of the data provider who provided the data to NCTC to make determinations regarding the Freedom of Information Act and first-party access under the Privacy Act, and discovery or other requests for such information in any legal proceeding, unless a different arrangement was agreed upon between NCTC and the data provider and specified in the Terms and Conditions or is required by law. Information derived from an operational file exempted from search and review, publication, and disclosure under 5 U.S.C. § 552 in accordance with law shall remain under the control of the data provider and be handled as coordinated in advance with the data provider and as specified in the Terms and Conditions for that information.

I. Baseline Safeguards, Procedures, and Oversight Mechanisms. During the temporary retention period, the IC element shall adhere to the following baseline

UNCLASSIFIED

safeguards, procedures, and oversight mechanisms for any dataset disseminated by NCTC under this Appendix:

1. The data will be maintained in a secure, restricted-access repository.
2. Access to the data will be limited to those IC element personnel, who: (i) access the data for the purpose authorized in section IV.A; (ii) are acting under, and agree to abide by, the IC element's information sharing and use rules, including this Appendix and the written agreement; (iii) have the requisite security clearance and a need-to-know in the course of their official duties; and (iv) have received the training required by section IV.D.
3. Access to the data will be monitored, recorded, and audited. This includes tracking of logons and logoffs, file and object manipulation and changes, and queries executed, in accordance with audit and monitoring standards applicable to the Intelligence Community. Audit records will be protected against unauthorized access, modifications, and deletion, and will be retained for a sufficient period to enable verification of compliance with the rules applicable to the data for which audit records apply.
4. The IC element's queries or other activities to assess information contained in the data disseminated pursuant to this Appendix shall be designed solely to identify information that is reasonably believed to constitute terrorism information.
5. The IC element shall query the data in a way designed to minimize the review of information concerning United States persons that does not constitute terrorism information. To identify information reasonably believed to constitute terrorism information contained in data disseminated pursuant to this Appendix, the IC element may conduct (i) queries that do not consist of, or do not consist exclusively of, terrorism data points, which are known or suspected terrorist identifiers or other pieces of terrorism information, and (ii) pattern-based queries and analyses. To the extent that these activities constitute "data mining" as that term is defined in the Federal Agency Data Mining Reporting Act of 2007, the IC element shall coordinate with NCTC to ensure proper reporting and to identify which element should report these activities as required by that Act.
6. The IC element will conduct compliance reviews as described below in section IX.

J. Enhanced Safeguards, Procedures, and Oversight Mechanisms. The IC element must also comply with any enhanced safeguards, procedures, and oversight mechanisms identified in the Terms and Conditions for the particular dataset or otherwise required by

UNCLASSIFIED

the Director of NCTC and specified in the written agreement signed by the IC element head or designee. See NCTC Guidelines, section III.C.3(e).

V. Dissemination of United States Person Information

A. General Dissemination Requirements.

1. *Terms and Conditions and Privacy Act.* All disseminations under this Appendix must be: (i) compatible with this Appendix; (ii) any applicable Terms and Conditions, and any other measures identified or specified in the written agreement or, if not compatible, the data provider must have otherwise consented to the dissemination; and (iii) permissible under the Privacy Act, 5 U.S.C. § 552a, if applicable.

2. *Dissemination to State, Local, or Tribal Authorities or Private-Sector Entities.* The NCTC Guidelines and this Appendix are not intended to alter or otherwise impact pre-existing information sharing relationships by federal agencies with state, local, or tribal authorities or private-sector entities, whether such relationships arise by law, Presidential Directive, MOU, or other formal agreement (including, but not limited to, those listed in section II of the NCTC Guidelines). To the extent that the NCTC Guidelines, this Appendix, and the written agreement allow for dissemination to state, local, tribal, or private sector entities, such dissemination will continue to be made, consistent with section 119(f)(1)(E) of the National Security Act (50 U.S.C. 404o(f)(1)(E)), in support of the Department of Justice (including the FBI) or the Department of Homeland Security responsibilities to disseminate terrorism information to these entities, and conducted under agreements with those Departments. This Appendix is not intended to, does not, and shall not be relied upon to create a grant of new or additional authority for information sharing with or dissemination of information to state, local, or tribal authorities or private-sector entities.

3. *Bulk Disseminations Prohibited.* In no case may the IC element make a further bulk dissemination of any dataset or any significant portion of a dataset. However, specific United States person information may be disseminated pursuant to the dissemination provisions in sections V.B or V.C below.

B. Basic Dissemination Requirements. The IC element may disseminate United States person information from datasets provided by NCTC if the General Dissemination Requirements are met, and if:

1. *Dissemination of Terrorism Information.* The United States person information reasonably appears to constitute terrorism information, or reasonably appears to be necessary to understand or assess terrorism information, and the IC element is disseminating the information to a federal, state, local, tribal, or foreign or international entity, or to any other appropriate entity or individual, that is

UNCLASSIFIED

reasonably believed to have a need to receive such information for the performance of a lawful function;

2. *Dissemination for Limited Purposes.* The United States person information is disseminated to other elements of the Intelligence Community or to a federal, state, local, tribal, or foreign or international entity, or to any other appropriate entity, for the limited purpose of assisting the IC element in determining whether the United States person information constitutes terrorism information. Before disseminating information under this paragraph, the IC element should consider approaching NCTC for this type of assistance. Any such recipients may only use the information for the limited purpose identified in this paragraph, and may not use the information for any other purpose or disseminate the information further without the prior approval of NCTC. Recipients of information under this paragraph must promptly provide the requested assistance to the IC element and promptly thereafter return the information to the IC element or destroy it unless the IC element authorizes continued retention after the specific information continued retention after the specific information is determined by the IC element to meet the dissemination criteria in section V.C of this Appendix. Recipients of information under this paragraph may not retain the information for continual assessment of whether it constitutes terrorism information unless such retention is permitted by the dissemination criteria in section V.C of this Appendix. This paragraph does not authorize the IC element to disseminate any bulk dataset or significant portion of a dataset believed to contain United States person information;

3. *Dissemination Based on Consent.* The United States person whom the information concerns consents to the dissemination; or

4. *Dissemination of Publicly Available Information.* The United States person information is publicly available.

C. Dissemination of Non-Terrorism Information. In addition, the IC element may disseminate United States person information contained in datasets provided by NCTC if that United States person information has been handled and subsequently identified in accordance with applicable safeguards and procedures,² if the General Dissemination Requirements are met, and if the United States person information:

1. Reasonably appears to be foreign intelligence or counterintelligence, or information concerning foreign aspects of international narcotics activities, or

² Note that this dissemination category does not authorize the IC element to search for additional categories of information, but rather allows the IC element to disseminate certain United States person information uncovered while performing counterterrorism analysis and searches in accordance with this Appendix, the applicable Terms and Conditions, and the written agreement.

UNCLASSIFIED

reasonably appears to be necessary to understand or assess foreign intelligence or counterintelligence or foreign aspects of international narcotics activities, and the IC element is disseminating the information to another federal, state, local, tribal, or foreign or international entity that is reasonably believed to have a need to receive such information for the performance of a lawful function, provided they agree to such further restrictions on dissemination as may be necessary;

2. Reasonably appears to be evidence of a crime, and the IC element is disseminating the information to another federal, state, local, tribal, or foreign agency that is reasonably believed to have jurisdiction or responsibility for the investigation or prosecution to which the information relates and a need to receive such information for the performance of a lawful governmental function;

3. Is disseminated to a Congressional Committee to perform its lawful oversight functions, after approval by the IC element's Office of General Counsel or senior legal advisor;

4. Is disseminated to a federal, state, local, tribal, or foreign or international entity, or to an individual or entity not part of a government, and is reasonably believed to be necessary to: (i) protect the safety or security of persons, property, or organizations; or (ii) protect against or prevent a crime or a threat to the national security, provided they agree to such further restrictions on dissemination as may be necessary;

5. Is disseminated to another federal, state, local, tribal, or foreign or international entity for the purpose of determining the suitability or credibility of persons who are reasonably believed to be potential sources or contacts, provided they agree to such further restrictions on dissemination as may be necessary;

6. Is disseminated to another federal, state, local, tribal, or foreign or international entity for the purpose of protecting foreign intelligence or counterintelligence sources and methods from unauthorized disclosure;

7. Is disseminated to other recipients, if the subject of the information provides prior consent in writing;

8. Is otherwise required to be disseminated by statutes; treaties; executive orders; Presidential directives; National Security Council directives; Homeland Security Council directives; or Attorney General-approved policies, memoranda of understanding, or agreements; or

9. Is disseminated to appropriate elements of the IC for the purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it.

UNCLASSIFIED

The identity of a United States person may be disseminated outside the Intelligence Community only if it is necessary or if it is reasonably believed it may become necessary to understand and assess such United States person information described above.

VI. Foreign Disseminations

For any dissemination of United States person information to a foreign or international entity, in addition to complying with the dissemination provisions of section V, the IC element must find that:

- A. the dissemination is consistent with the interests of the United States, including U.S. national security interests;
- B. the dissemination complies with DCID 6/6 or any successor ICD³;
- C. the foreign or international entity has agreed not to disseminate the information further without approval by the IC element; and
- D. the IC element, in consultation with its General Counsel or senior legal advisor, has considered the effect such dissemination may reasonably be expected to have on any identifiable United States person to determine whether any additional safeguards are needed.

VII. Retention of Information for Administrative Purposes

To the extent consistent with law, United States person information acquired pursuant to this Appendix may be retained if necessary to conduct the oversight, auditing, redress, or compliance activities required by these Guidelines, if required by law or court order to be retained, or if necessary to determine whether the requirements of these Guidelines or applicable laws are satisfied. Any information retained under this paragraph beyond the temporary retention period may not be used for purposes other than those specified in the preceding sentence and must be promptly removed from the IC element's systems once retention is no longer necessary or required for those purposes, except that the IC element may retain any oversight, audit, redress, or compliance records or reports in accordance with its records retention policies.

VIII. The IC Element's Computer Systems

In designing its computer systems, the IC element shall take reasonable steps to enhance its ability to monitor activity involving United States person information and other sensitive information, and to facilitate compliance with, and the auditing and reporting required by, this Appendix.

³ ICD 403 is currently in draft. Once signed, any foreign dissemination would be required to comply with ICD 403 and any implementing IC Policy Guidance and IC Standards.

IX. Oversight and Compliance

A. Subject to oversight by the IC element's Civil Liberties and/or Privacy Officer, if applicable, and the ODNI Civil Liberties Protection Officer, the IC element shall conduct periodic reviews to verify continued compliance with this Appendix, including compliance with any Terms and Conditions and any measures specified in the written agreement. These reviews shall include spot checks, reviews of audit logs, and other appropriate measures.

B. The IC element, in coordination with the IC element's Civil Liberties and/or Privacy Officer (or other appropriate official as identified in the written agreement), shall conduct periodic reviews of its continued need for access to each dataset disseminated pursuant to the NCTC Guidelines and this Appendix to determine whether such access remains necessary and appropriate. In conducting this review, consideration shall be given to the purpose for which the dataset was disseminated; the success of that dataset in fulfilling legitimate counterterrorism purposes; whether those purposes can now be fulfilled through the use of other data in the IC element's possession, or through other appropriate means; and privacy and civil liberties considerations applicable to the particular dataset.

C. The IC element shall promptly report, in writing, to the IC element head, the Director of NCTC, the ODNI General Counsel, the ODNI Civil Liberties Protection Officer, the Department of Justice, and the IC Inspector General upon discovery of any significant failure to comply with (i) this Appendix; (ii) baseline or enhanced safeguards, procedures, or other oversight mechanisms; or (iii) any Terms and Conditions or the written agreement. For the purposes of this Appendix, a "significant failure" is a failure that constitutes a violation of the Constitution, or other law, including any executive order, and/or a failure that leads to unauthorized access, use, or dissemination of personally identifiable information about a United States person. NCTC shall then report to any data provider whose information was affected by the noncompliance, in accordance with the Terms and Conditions for that data.

D. The IC element shall report annually in writing to the IC element head and to the ODNI Civil Liberties Protection Officer on the measures that the IC element is taking to ensure that its access to, and retention, use, and dissemination of, United States person information is appropriate under this Appendix, and in compliance with all Terms and Conditions and written agreement. The report shall include:

1. The results of the review required in section IX.B. above, regarding whether access to the bulk dataset continues to be appropriate;
2. A general description of the IC element's compliance and audit processes;

UNCLASSIFIED

3. A description of the audits, spot checks, and other reviews the IC element conducted during the previous year, and the results of those audits, spot checks or other reviews, to include any shortcomings identified;
4. A description of how the IC element ensures that it promptly purges United States person information that does not meet the standards for retention under this Appendix, related Terms and Conditions, and any other measures specified in the written agreement;
5. An assessment of the United States person information disseminated by the IC element directly to foreign, international, state, local, tribal, or private sector entities or individuals; the restrictions, if any, that the IC element imposed on the entities' use or further dissemination of such information; and any known misuse of such information by a recipient, data breach, or significant failure by the recipient to comply with the terms of the certification required under section VI.C of this Appendix;
6. An assessment of whether there is a need for enhanced safeguards, procedures, or oversight regarding the handling of United States person information or other sensitive information, or any other reasonable measures that should be taken to improve the handling of information;
7. Measures the IC element has taken to comply with the requirements of section VIII with respect to its computer systems; and
8. A description of any material changes or improvements the IC element implemented, or is considering implementing, to improve compliance with this Appendix.

E. The IC element shall provide a copy of this report to the IC element General Counsel, the IC element Civil Liberties and/or Privacy Officer, the Director of NCTC, the ODNI General Counsel, the IC element's Inspector General, and the IC Inspector General, and shall make the report available upon request to the Assistant Attorney General for National Security. The IC element shall also make available to the IC element's Inspector General and the IC Inspector General any other reports or documentation necessary to ensure compliance with this Appendix.

F. The reporting required by this Appendix does not replace any other reporting required by statute, executive order, or regulation.

X. Interpretation and Departures

A. The IC element shall refer all questions relating to the interpretation of these Guidelines to the IC element's Office of General Counsel or other senior legal advisor. The IC element's General Counsel shall consult with the ODNI General Counsel regarding any novel or significant interpretations, and the ODNI General Counsel shall

UNCLASSIFIED

then consult with the Assistant Attorney General for National Security to the extent required by the NCTC Guidelines.

B. The ODNI General Counsel and the Assistant Attorney General for National Security must approve in advance any departures from this Appendix. If there is not time for such approval and a departure from this Appendix is necessary because of the immediacy or gravity of a threat to the safety of persons or property or to the national security, the IC element head, other senior IC element personnel identified in the written agreement with NCTC, the Director of NCTC, or the NCTC Director's senior representative present may approve a departure from these Guidelines. The ODNI General Counsel shall be notified as soon thereafter as possible. The ODNI General Counsel shall provide prompt written notice of any such departures to the Assistant Attorney General for National Security. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States.

XI. Status as Internal Guidance

The provisions in this Appendix are set forth solely for the purpose of internal IC element and ODNI guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law or in equity, by any party in any matter, civil or criminal, nor do they place any limitation on otherwise lawful investigative and litigation prerogatives of the U.S. Government.