

**INFORMATION PAPER: DESCRIPTION OF CIVIL LIBERTIES AND PRIVACY PROTECTIONS INCORPORATED  
IN THE UPDATED NCTC GUIDELINES  
JANUARY 2013**

In March, 2012, the Director of National Intelligence (DNI), the Attorney General, and the Director of the National Counterterrorism Center (NCTC) approved the updated *Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information* (referred to here as the "NCTC Guidelines" or "Guidelines") (available at [www.nctc.gov](http://www.nctc.gov)). The NCTC Guidelines make important updates and modifications to the 2008 version of the Guidelines. The new Guidelines ensure that NCTC has an effective and efficient means of assessing federal agency datasets that are likely to contain significant terrorism information, permit NCTC to use terrorism information for proper purposes subject to multi-layered privacy and civil liberties protections, and establish comprehensive compliance and oversight mechanisms.<sup>1</sup>

**BACKGROUND AND SUMMARY**

Congress established the National Counterterrorism Center (NCTC) within the Office of the Director of National Intelligence (ODNI) to integrate and analyze all intelligence possessed or acquired by the United States Government pertaining to terrorism, and to ensure that all agencies with a counterterrorism mission have access to that intelligence to perform their duties. In November, 2008, the DNI and the Attorney General approved guidelines governing how NCTC identifies terrorism information in datasets that other federal agencies have already lawfully obtained pursuant to their own authorities, and prescribing protections for the information to be shared with NCTC (the 2008 Guidelines). The 2008 Guidelines established three "tracks" for NCTC to access or acquire such information from other federal agencies. Under Track 1, NCTC analysts would have account-based access to a relevant agency dataset, while under Track 2, NCTC would submit query terms for the providing agency to perform the search and return responsive information. Under Track 3, the agency dataset would be replicated (copied) at NCTC so

**About this Information Paper.** The ODNI's Civil Liberties and Privacy Office (CLPO) has prepared this information paper to describe the civil liberties and privacy protections incorporated in the NCTC Guidelines. This paper furthers one of the main goals under CLPO's *Civil Liberties and Privacy Enterprise Strategy*, to provide appropriate transparency to mission partners, oversight bodies, Congress, and the American public into the Intelligence Community's (IC's) civil liberties and privacy protections. CLPO is led by the "Civil Liberties Protection Officer," a position established by Section 103D of the National Security Act of 1947. Statutory duties of the Civil Liberties Protection Officer include ensuring that the protection of civil liberties and privacy is appropriately incorporated in the policies and procedures of IC elements, and overseeing compliance by the ODNI with requirements under the Constitution and all laws, regulations, Executive orders, and implementing guidelines relating to civil liberties and privacy. For more information, visit the CLPO page on [www.dni.gov](http://www.dni.gov).

NCTC could use its analytic tools to identify terrorism information; if NCTC could not "promptly" identify terrorism information in the replicated dataset, the 2008 Guidelines required NCTC to "promptly remove" the information. As implemented at NCTC, this generally required the removal of information within 180 days.

Reviews conducted in the aftermath of the December 25, 2009 terrorist attack found that the federal counterterrorism community had failed to

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
CIVIL LIBERTIES AND PRIVACY OFFICE

adequately identify, correlate, and fuse together the discrete pieces of intelligence available in different databases. As a result, the President directed, among other things, that enhancements be pursued to improve knowledge discovery, database integration, cross-database searches, and the ability to correlate biographic information with terrorism intelligence.<sup>2</sup> In pursuing such changes, and in light of its operational experience, NCTC recognized it needed to retain replicated datasets for longer periods to identify previously unknown relationships to terrorism information, which might become evident only after time-consuming correlation with other datasets, or with the discovery of new information at later points in time.

In March, 2012, the DNI, the Attorney General, and the Director of NCTC approved the updated NCTC Guidelines. The Guidelines now provide that datasets likely to contain significant terrorism information may be temporarily retained for up to 5 years (or a shorter period as determined with the providing agency, known as the "data provider"). The updated Guidelines carry forward the same three-track framework from the 2008 Guidelines, while adding specificity on how data is obtained, retained, and disseminated, and providing for enhanced safeguards and oversight mechanisms to protect important privacy and civil liberties interests throughout the information sharing lifecycle.

### Highlights of Protective Provisions:

**Federal information.** The Guidelines apply only to information that is lawfully in the possession of other federal government agencies and can be legally shared with NCTC, in accordance with applicable laws, regulations, executive orders, and international obligations.

**“Reasonable belief” standard.** The Guidelines only apply to datasets that are reasonably believed to contain terrorism information. Moreover, NCTC may only retain United States person information (and other information protected under the Guidelines) within such datasets beyond the temporary retention period if it is reasonably believed to constitute terrorism information.

**Dataset-specific protections.** Specific protections, including the length of the temporary retention period, will be documented in “Terms and Conditions” by NCTC and the agency providing the data to accommodate any additional privacy or civil liberties concerns, international obligations, and similar considerations.

**Protections by track.** For Tracks 1 and 2, NCTC’s initial query term must itself be an item of terrorism information. For Track 3, NCTC’s queries must be designed solely to identify terrorism information and to minimize the review of information protected under the Guidelines that is not terrorism information. In addition, NCTC must limit access to duly trained and authorized personnel, implement compliance verification measures, and determine whether to apply enhanced safeguards (e.g., more data access/use restrictions). For all tracks, information protected under the Guidelines may be shared only under limited circumstances.

**Oversight and Compliance.** The Guidelines require periodic compliance reviews, compliance reporting, and oversight by CLPO, ODNI’s Office of General Counsel (ODNI/OGC), the Intelligence Community Inspector General (ICIG), and the Privacy and Civil Liberties Oversight Board. Compliance reports must be made available to DOJ. NCTC’s compliance is also subject to congressional oversight.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
CIVIL LIBERTIES AND PRIVACY OFFICE

**DETAILED DESCRIPTION**

The following section presents a detailed description of the Guidelines' provisions relating to privacy and civil liberties protections, with citations in footnotes to the relevant sections of the Guidelines, to facilitate review.

1. **The NCTC Guidelines implement NCTC's authorities under applicable laws and Executive orders.** The NCTC Guidelines were established to implement certain of NCTC's authorities to integrate and analyze all intelligence possessed or acquired by the United States Government pertaining to terrorism, and to ensure that all agencies with a counterterrorism mission have access to that intelligence to perform their duties.<sup>3</sup>
2. **The Guidelines apply only to datasets that are lawfully in the possession of the federal government.** The Guidelines apply only to datasets that have already been lawfully collected by, and are in the possession of, other federal departments and agencies. The Guidelines do not provide any new authorities for the government to collect information, and do not authorize NCTC to acquire information directly from the private sector.<sup>4</sup>
3. **Only federal agency datasets that are reasonably believed to contain terrorism information may be shared with NCTC.** The only federal datasets that NCTC may access under the Guidelines are those that NCTC determines, in coordination with the department or agency that maintains the dataset, are "reasonably believed to contain terrorism information."<sup>5</sup> For datasets to be replicated at NCTC under Track 3, the Director of NCTC, in coordination with the data provider, must first make a finding that the dataset is "likely to contain significant terrorism information."<sup>6</sup>
4. **Datasets may only be shared to the extent consistent with applicable laws, regulations, executive orders, and international obligations.** The Guidelines provide that NCTC will access, acquire, retain, use and disseminate

information, including United States person information,<sup>7</sup> pursuant to the standards of Executive Order 12333, consistent with the National Security Act of 1947, as authorized by law or regulations, including privacy laws,<sup>8</sup> and in accordance with international agreements (discussed in Paragraph 5 below).

- Under Executive Order 12333, IC elements are required to have guidelines approved by the head of the IC element and the Attorney General, in consultation with the DNI, for the collection, retention, and dissemination of information concerning United States persons.<sup>9</sup> The Guidelines therefore refer explicitly to the protection of U.S. person information. As described in Paragraph 5 below, the Guidelines also require the protection of other information.
  - NCTC's access to a dataset must be consistent with the Privacy Act, including the routine uses set forth in the System of Records Notice under which the data was originally collected and maintained by the data provider.<sup>10</sup>
  - As described in Paragraph 7 below, the Guidelines require NCTC to work with the data provider to identify the legal, regulatory, and policy constraints and requirements that apply to the sharing arrangement, and to document them in the Terms and Conditions that will govern NCTC's access and use of the dataset.<sup>11</sup>
5. **The NCTC Guidelines expressly require that international agreements be honored.** The Guidelines explicitly acknowledge that NCTC must adhere to and honor the terms of any international agreement pursuant to which a data provider has received access to data. Specifically, the Guidelines require that NCTC consult with the data provider to identify and put in place additional measures as necessary to honor obligations under applicable international agreements and interests of foreign governments.<sup>12</sup> These measures will be included in the Terms and Conditions that govern NCTC's access to each particular

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
CIVIL LIBERTIES AND PRIVACY OFFICE

dataset.<sup>13</sup> Accordingly, under the requirements of the Guidelines, information pertaining to non-United States persons is subject to protection in accordance with applicable international obligations and Terms and Conditions.<sup>14</sup>

6. **The standard for identifying “terrorism information” within a dataset is “reasonable belief.”** NCTC may retain United States person information (and other information protected under the Guidelines, as applicable) beyond the temporary retention period, and use it to carry out NCTC’s counterterrorism mission, if it is “reasonably believed to constitute terrorism information.”<sup>15</sup> The Guidelines provide that 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.<sup>16</sup>

7. **NCTC must work with the federal departments and agencies maintaining relevant datasets to jointly determine whether and how a dataset is to be accessed or acquired.** Under the Guidelines, NCTC will work with the data provider to identify any legal constraints, operational considerations, privacy or civil rights or civil liberties concerns or protections, or other issues, and to incorporate those considerations into the Terms and Conditions that will provide additional protections for NCTC’s access to or acquisition of a dataset under the Guidelines.<sup>17</sup>

- The Terms and Conditions are intended to ensure that the 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) comports with applicable laws, regulations, guidelines and instructions.<sup>18</sup> NCTC and the data provider are to document, in the

Terms and Conditions, any additional protections and requirements beyond those set forth in the Guidelines, including safeguards, procedures, oversight mechanisms, and protections for foreign government interests, privacy and civil liberties, and similar considerations that apply to the use of the information.<sup>19</sup>

- The Terms and Conditions should also reflect measures to honor obligations under international agreements, and to reflect the degree of advance coordination, if any, for disseminating information.<sup>20</sup>
- These Terms and Conditions supplement the protections of the Guidelines,<sup>21</sup> but cannot contravene the Privacy Act. As such, sharing of data with NCTC must be consistent with the routine uses provided for in the System of Records Notice under which the data was first collected by the data provider.<sup>22</sup>
- Compliance with the Terms and Conditions is included in the compliance and oversight sections of the Guidelines.<sup>23</sup>

8. **Respect for First Amendment-protected activities.** The Guidelines prohibit access, acquisition, retention, use, or dissemination of U.S. person information solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other legal rights.<sup>24</sup>

9. **NCTC must implement information accuracy and error correction measures.** The Guidelines prohibit NCTC from retaining, using or disseminating information protected under the Guidelines that has been erroneously provided to it, and require the prompt removal of such information from NCTC systems.<sup>25</sup> They also require that NCTC promptly correct information in its systems found to contain errors, and that it notify the data provider of such errors.<sup>26</sup>

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
CIVIL LIBERTIES AND PRIVACY OFFICE

- In addition, the Guidelines require that NCTC and the data provider establish procedures to ensure that the data provider notifies NCTC of any information the data provider believes or subsequently determines to be materially inaccurate or unreliable, with NCTC required to implement mechanisms to correct or document such inaccuracy or unreliability, and to supplement incomplete information to the extent additional information becomes available.<sup>27</sup>
- The Guidelines further provide that NCTC and the data provider will work together to ensure that data is updated and verified while it is retained by NCTC, in accordance with the data quality, data notice, and redress provisions of the ODNI ISE Privacy Instruction.<sup>28</sup>

**10. The Guidelines provide specific protections for each “track” of access.** The protections for Tracks 1 and 2—which are very similar to the provisions applicable to those tracks in the 2008 Guidelines—are described below; Track 3 protections are described in the next paragraph.

- Track 1. For Track 1 – account-based access - the Guidelines provide that NCTC will access such datasets only for the purpose of identifying terrorism information; if information acquired by NCTC under this track is subsequently determined not to constitute terrorism information, NCTC must promptly purge the information from its systems.<sup>29</sup> The Guidelines further provide that the initial query term used in such access shall be a known or suspected terrorist identifier or other piece of terrorism information (“terrorism datapoints”), and that while NCTC may follow up on positive query results to explore a known or suspected terrorist’s network of contacts or supports, its activities must be “designed to identify information that is reasonably believed to constitute terrorism information.”<sup>30</sup>

- Track 2. Track 2 involves submitting query terms to the data provider. The Guidelines include similar protections to those described above: the query terms must consist of terrorism datapoints; if information returned by the data provider is not terrorism information, it must be purged; and NCTC’s activities must be designed to identify information that is reasonably believed to be terrorism information.<sup>31</sup>

**11. The Guidelines establish a series of safeguards for federal agency datasets replicated at NCTC under Track 3.** The Guidelines establish detailed protections under Track 3.

- Protections during identification and acquisition of datasets. Before acquiring a dataset under Track 3, the Guidelines require that the Director of NCTC, in coordination with the data provider, make a finding that the dataset is “likely to contain significant terrorism information” and that NCTC’s purposes “cannot effectively be served through Tracks 1 or 2.”<sup>32</sup> The NCTC Director must also consider whether NCTC’s purposes can be served by replicating a portion of the dataset, such as through limiting the types of records, or the number of fields that NCTC is given access to.<sup>33</sup> As previously noted, NCTC and the data provider must also establish Terms and Conditions specifying dataset-specific protections, including the temporary retention period, which cannot exceed five years, but may be shorter if required by law, executive order or regulation, or if determined to be appropriate in coordination with the data providing agency.<sup>34</sup> NCTC is required to use reasonable measures to identify and mark or tag United States person information in the datasets.<sup>35</sup>
- Baseline safeguards. During temporary retention, the data is subject to a number of baseline safeguards. The datasets must be



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
CIVIL LIBERTIES AND PRIVACY OFFICE

maintained in a secure, restricted-access repository.<sup>36</sup> NCTC must limit access to only those NCTC personnel with a mission need for the information, who have received training on (and are operating under) the Guidelines (and any specific requirements relating to the dataset).<sup>37</sup> NCTC must also ensure that access to and use of these datasets are subject to monitoring, recording and auditing measures, and that audit records are protected from unauthorized access or modification and are retained for sufficient periods to enable verification of compliance.<sup>38</sup> In addition, a key baseline safeguard is the requirement that NCTC's analytic activities must be designed solely to identify information that is reasonably believed to constitute terrorism information, and also to minimize the review of information protected under the Guidelines that does not constitute terrorism information.<sup>39</sup>

- Enhanced safeguards. Moreover, for each dataset, the Director of NCTC must determine, in consultation with the ODNI General Counsel and the ODNI Civil Liberties Protection Officer, whether additional enhanced safeguards should be applied (such as additional access/use/dissemination restrictions; privacy-enhancing technologies; data segregation; or more frequent reviews of policies/practices).<sup>40</sup> NCTC must consider a number of factors in making such a determination, including any recommendations for enhanced safeguards made by the data provider.<sup>41</sup>
- Pattern-based queries. The Guidelines provide that, “[t]o identify information reasonably believed to be terrorism information contained in Track 3 data, NCTC may conduct ... pattern-based queries and analyses.”<sup>42</sup> However, NCTC must still satisfy the requirement that queries be designed solely to identify information reasonably believed to be terrorism information, and to minimize the

review of information protected under the Guidelines that is not terrorism information.<sup>43</sup> In addition, to the extent any pattern-based queries constitute "data mining" as defined by the Data Mining Reporting Act of 2007, NCTC would be required to report this activity to Congress, together with a description of the applicable safeguards.<sup>44</sup>

- Periodic Review of the Need For Continued Track 3 Access. The Guidelines require NCTC to conduct periodic reviews of all Track 3 datasets, in coordination with CLPO, to determine whether continued Track 3 access remains appropriate. In conducting these reviews, consideration is to be given to the purpose for which Track 3 access was initially chosen, whether that purpose has in fact been fulfilled through Track 3 access, and whether such purposes might now be fulfilled through Tracks 1 or 2 (as well as other relevant privacy and civil liberties considerations applicable to the dataset being reviewed).<sup>45</sup>
  - Removal of information. The Guidelines require NCTC to remove from its systems all information identified as protected under the Guidelines, that NCTC does not reasonably believe constitutes terrorism information within the prescribed time periods (five years or shorter, as established by the Terms and Conditions), unless removal is prohibited by applicable legal requirements or by regulation or policy approved by the Attorney General.<sup>46</sup>
12. **NCTC must provide comprehensive training.** NCTC must ensure that NCTC personnel who are provided access to datasets under the Guidelines receive training to ensure that they use the datasets only for authorized purposes, understand the baseline and enhanced safeguards, dissemination restrictions, and other privacy and civil liberties protections that apply to each dataset. The training must be refreshed annually.<sup>47</sup>

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
CIVIL LIBERTIES AND PRIVACY OFFICE

13. **The Guidelines govern – and restrict – how information can be disseminated.** The Guidelines define “dissemination” broadly, to mean “transmitting, communicating, sharing, passing, or providing access to information outside NCTC by any means, to include oral, electronic, or physical means.”<sup>48</sup>

- Terms and Conditions and Privacy Act. All disseminations must be consistent with the Terms and Conditions agreed upon with the other agency (or otherwise with the data provider’s consent), and with applicable laws, including the Privacy Act.<sup>49</sup>
- Terrorism information. Once NCTC has determined that information is “terrorism information,” it may disseminate the information to entities authorized to receive that information.<sup>50</sup>
- Disseminations for a limited purpose. In addition, the Guidelines provide that information acquired under Tracks 1, 2, or 3 may be disseminated for the limited purpose of assisting NCTC in evaluating whether the information is terrorism information. This provision mandates a series of specific safeguards and oversight controls designed to ensure that the recipient uses its access to the data solely to provide NCTC the assistance requested, and only for the duration necessary to provide that assistance.<sup>51</sup>
- "Standard" dissemination under Track 3. The Guidelines address circumstances under which NCTC may disseminate information it comes across when it conducts authorized queries for terrorism information.<sup>52</sup> For example, if an analyst enters a query seeking to identify terrorism information, and in the information that is responsive to that query, identifies information that constitutes evidence of a crime (or fits within another such specified category), the Guidelines permit NCTC to disseminate that information in accordance with the applicable provisions of the Guidelines.<sup>53</sup> The Guidelines explicitly state that these provisions do not authorize NCTC to search for these categories of

information; thus, NCTC remains bound by the Guidelines’ requirements that it query Track 3 datasets only for terrorism information.<sup>54</sup> In any event, identities of U.S. persons may be disseminated outside the IC only to the extent necessary to understand the underlying information being disseminated.<sup>55</sup>

- “Bulk” dissemination under Track 3. The Guidelines include specific restrictions on any proposed dissemination of data that has not yet been determined to be terrorism information. It is important to recall that under the Guidelines, “dissemination” is defined to include “providing access” to the information. Any such dissemination would have to be consistent with applicable laws (including the Privacy Act), international obligations, and executive orders; would require approvals and consultations involving senior officials at NCTC, ODNI, and DOJ; and would, in addition, require the data provider to expressly agree to the dissemination.<sup>56</sup> Moreover, the recipient would have to expressly agree, in writing, to apply safeguards and oversight controls in the Guidelines.
- Foreign disseminations. Any disseminations involving a foreign government or entity would, in addition to all the foregoing limitations, be subject to further safeguards (e.g., a determination of whether additional safeguards are needed based on potential impact of the dissemination on any identifiable U.S. person).<sup>57</sup>

14. **The Guidelines specify compliance and oversight mechanisms to verify that NCTC is properly following the provisions of the Guidelines and applicable Terms and Conditions.** NCTC activities already receive review and oversight from the ODNI Civil Liberties Protection Officer, ODNI/OGC, and the IC Inspector General (ICIG). In addition, NCTC has a full-time on-site Civil Liberties and Privacy Officer. NCTC is required to

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
CIVIL LIBERTIES AND PRIVACY OFFICE

report violations of law and executive order to the Intelligence Oversight Board of the President's Intelligence Advisory Board. NCTC is also subject to the oversight of the Privacy and Civil Liberties Oversight Board, and must keep the intelligence committees in Congress fully and currently informed of its activities. The Guidelines build on this existing oversight structure.

- The Guidelines designate the Director of NCTC, in consultation with the ODNI Office of General Counsel (OGC), as the responsible official for ensuring compliance with the Guidelines, and establish that CLPO is responsible for overseeing such compliance.<sup>58</sup>
- The Guidelines require NCTC to conduct periodic compliance reviews under CLPO oversight (such as spot checks and reviews of audit logs),<sup>59</sup> and to consult with OGC and CLPO on implementation.<sup>60</sup>
- NCTC must also periodically re-assess whether continued temporary retention of data under Track 3 remains appropriate.<sup>61</sup>
- The Guidelines provide for various types of compliance reporting, including reporting significant failures to comply with applicable requirements, and a comprehensive annual compliance report, all of which are made available to CLPO, OGC, the Department of Justice, and the ICIG.<sup>62</sup> Compliance reports are also submitted to the data provider as called for by applicable Terms and Conditions.<sup>63</sup>
- Finally, the Guidelines provide that the Privacy and Civil Liberties Oversight Board will have access to all relevant NCTC material and will have the opportunity to conduct oversight in accordance with its statutory mission.<sup>64</sup>



## ENDNOTES

---

<sup>1</sup> The NCTC Guidelines use the statutory definition of “terrorism information” in Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, 6 U.S.C. section 485(a)(5): “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).

<sup>2</sup> For example, see Summary of White House Review of December 25, 2009 Attempted Terrorist Attack, available at <http://www.whitehouse.gov/the-press-office/white-house-review-summary-regarding-12252009-attempted-terrorist-attack>; and Administration of President Barack Obama, Attempted Terrorist Attack of December 25, 2009: Intelligence, Screening, and Watchlisting Corrective Actions, January 10, 2010, Daily Comp. Pres. Docs., 2010 DCPD No. 00009, available at <http://www.gpo.gov/fdsys/pkg/DCPD-201000009/pdf/DCPD-201000009.pdf>.

<sup>3</sup> In general, see section 119 of the National Security Act of 1947, 50 U.S.C. section 404o. Note that Section 119(a) establishes that NCTC is part of the Office of the Director of National Intelligence (ODNI). Section 119(e) and section 119(f)(1)(E) of the National Security Act of 1947 in turn provide that NCTC is to carry out certain of its duties under “guidelines referred to in Section 102A(b)” of the Act. Section 102A(b) provides that “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.”

<sup>4</sup> The Guidelines were established to govern how NCTC accesses, retains, uses, and disseminates terrorism information that is contained within datasets maintained by other executive departments or agencies that are identified as including non-terrorism information. NCTC Guidelines, section I.C.

<sup>5</sup> NCTC Guidelines, section III.B.1.

<sup>6</sup> NCTC Guidelines, section III.C.3(b).

<sup>7</sup> Section I.B. of the Guidelines provides that the term “United States person” is as defined in Executive Order 12333, which provides that a *United States person* 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.” Executive Order 12333, Section 3.5(k).

<sup>8</sup> NCTC Guidelines, section III.A.4(a).

<sup>9</sup> In particular, Section 2.3 of Executive Order 12333 requires procedures approved by the head of the IC element and the Attorney General, in consultation with the DNI, to specify how the element will collect, retain, and disseminate information concerning United States persons.

<sup>10</sup> Information subject to the Privacy Act that is maintained by NCTC is subject to NCTC’s Privacy Act responsibilities, as applicable. For example, see Privacy Act System of Records Notice for NCTC Knowledge Repository, 76 F.R. 42747, available at [http://www.dni.gov/files/documents/FR\\_Vol%2076\\_No%20138\\_Notice\\_20110719.pdf](http://www.dni.gov/files/documents/FR_Vol%2076_No%20138_Notice_20110719.pdf).

<sup>11</sup> NCTC Guidelines, section III.B.2.

<sup>12</sup> NCTC Guidelines, section III.B.2(b) and (c). See discussion below for more information on Terms and Conditions.

<sup>13</sup> Moreover, NCTC may implement “enhanced safeguards” to address dataset-specific considerations pertaining to international obligations (enhanced safeguards are further discussed below). NCTC Guidelines, section III.C.3(e). Note that, in setting forth the process for resolving a dispute between NCTC and the data provider regarding NCTC’s access

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
CIVIL LIBERTIES AND PRIVACY OFFICE

---

to a dataset or the Terms and Conditions, the Guidelines specifically include, as an example, a concern that the Terms and Conditions “are not in accordance with ... international agreements.” NCTC Guidelines, section III.B.2(d).

<sup>14</sup> In addition, note that the Guidelines require that NCTC follow ODNI’s information sharing privacy policy (described in endnote 18 below), which explicitly acknowledges that the information within its scope includes not only United States person information, but also “information designated by executive order, international agreement or other instrument as subject to information privacy or other protections.”

<sup>15</sup> NCTC Guidelines, section III.A.2.

<sup>16</sup> NCTC Guidelines, section III.A.2.

<sup>17</sup> NCTC Guidelines, section III.B.2(a).

<sup>18</sup> NCTC Guidelines, section III.B.2. An “instruction” is internal ODNI policy. Section III.B.2 and Section II.r specifically refer to ODNI Instruction 80.05, Implementation of Information Sharing Environment Privacy Guidelines for Sharing Protected Information (<http://www.dni.gov/files/documents/ODNI%20ISE%20Privacy%20Guidelines.pdf>). This Instruction implements within ODNI (and NCTC) the 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, which were issued by the President in 2006 pursuant to Section 1016 of the IRTPA (<http://www.ise.gov/sites/default/files/PrivacyGuidelines20061204.pdf>).

<sup>19</sup> NCTC Guidelines, section III.B.2(c).

<sup>20</sup> NCTC Guidelines, sections III.B.2(b) and (c).

<sup>21</sup> NCTC Guidelines, section III.B.2(a) (providing that the Terms and Conditions incorporate the Guidelines by reference).

<sup>22</sup> During the temporary retention period for assessment by NCTC, Track 3 data is maintained by NCTC under its System of Records Notice (SORN) ODNI/NCTC-004, “National Counterterrorism Center Knowledge Repository,” 76 FR 42747; FR Doc. No. 2011-18193.

<sup>23</sup> NCTC Guidelines, section VI. If NCTC and the data provider cannot agree on (i) providing the information, (ii) the “track” through which NCTC will access the data, or (iii) the Terms and Conditions, then the Guidelines provide for a process by which either side’s objections can be escalated, addressed and resolved. If the heads of each agency cannot resolve a dispute, then constitutional or other legal matters are referred to the Attorney General, and other disputes are addressed through the National Security Council process. The Guidelines list, as examples of possible objections, a belief that the Terms and Conditions do not adequately ensure the protection of privacy and civil liberties, or that sharing is inconsistent with applicable laws, international agreements, and regulations. NCTC Guidelines, section III.B.2(d).

<sup>24</sup> NCTC Guidelines, section III.A.4(b).

<sup>25</sup> NCTC Guidelines, section III.A.3.

<sup>26</sup> NCTC Guidelines, section III.A.3.

<sup>27</sup> NCTC Guidelines, section III.B.2.

<sup>28</sup> NCTC Guidelines, section III.B.2. See also endnote 18 above.

<sup>29</sup> NCTC Guidelines, section III.C.1(b).

<sup>30</sup> NCTC Guidelines, section III.C.1(c).

<sup>31</sup> NCTC Guidelines, section III.C.2(b).

<sup>32</sup> NCTC Guidelines, section III.C.3(b).

<sup>33</sup> NCTC Guidelines, section III.C.3(b).

<sup>34</sup> NCTC Guidelines, section III.C.3(c).

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
CIVIL LIBERTIES AND PRIVACY OFFICE

---

<sup>35</sup> NCTC Guidelines, section III.C.3(c).

<sup>36</sup> NCTC Guidelines, section III.C.3(d)(1).

<sup>37</sup> NCTC Guidelines, section III.C.3(d)(2).

<sup>38</sup> NCTC Guidelines, section III.C.3(d)(3).

<sup>39</sup> NCTC Guidelines, section III.C.3(d)(4).

<sup>40</sup> NCTC Guidelines, section III.C.3(e).

<sup>41</sup> NCTC Guidelines, section III.C.3(e).

<sup>42</sup> NCTC Guidelines, section III.C.3(d)(4).

<sup>43</sup> NCTC Guidelines, section III.C.3(d)(4).

<sup>44</sup> NCTC Guidelines, section III.C.3(d)(4). The 2010 ODNI Data Mining Report to Congress described the NCTC “Datasphere” program, which at that time envisioned the potential future inclusion of a data mining capability. As subsequently reported in ODNI’s 2011 Data Mining Report, NCTC terminated the Datasphere program without developing such a capability. These reports are available on ODNI/CLPO’s website, at <http://www.dni.gov/index.php/about/organization/civil-liberties-privacy-office-reports>

<sup>45</sup> NCTC Guidelines, section VI.B.

<sup>46</sup> NCTC Guidelines, section III.C.3(f). Information may continue to be retained for “administrative purposes” only as provided in NCTC Guidelines, section V- as necessary to conduct oversight, auditing, redress or compliance activities required by the Guidelines; if retention is required by law or court order; or if necessary to determine if applicable requirements are satisfied.

<sup>47</sup> NCTC Guidelines, section III.B.3.

<sup>48</sup> NCTC Guidelines, section IV.A.1

<sup>49</sup> NCTC Guidelines, section III.A.4, and section IV.A.2.

<sup>50</sup> NCTC Guidelines, section IV.B.1. NCTC may also disseminate information with the consent of the person to whom the information pertains, and may disseminate publicly available information. NCTC Guidelines, section IV.B.3 and 4.

<sup>51</sup> NCTC Guidelines, section IV.B.2.

<sup>52</sup> NCTC Guidelines, section IV.C.

<sup>53</sup> Executive Order 12333, Section 2.3, authorizes the dissemination of these categories of information in accordance with procedures established by the head of the Intelligence Community element concerned and approved by the Attorney General, in consultation with the DNI.

<sup>54</sup> NCTC Guidelines, section IV.C, footnote 3.

<sup>55</sup> NCTC Guidelines, section IV.C (unnumbered paragraph at end of section). For disseminations within the IC, it should be noted that IC elements would apply their applicable collection, retention, and dissemination procedures under Executive Order 12333 to any such United States person information.

<sup>56</sup> See generally, NCTC Guidelines, section IV.C.2.

<sup>57</sup> NCTC Guidelines, section IV.D.

<sup>58</sup> NCTC Guidelines, section III.A.5.

<sup>59</sup> NCTC Guidelines, section VI.A.

<sup>60</sup> NCTC Guidelines, section III.A.4(b).

<sup>61</sup> NCTC Guidelines, section VI.B.

<sup>62</sup> NCTC Guidelines, section VI.D.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
CIVIL LIBERTIES AND PRIVACY OFFICE

---

<sup>63</sup> NCTC Guidelines, section VI.D.1.

<sup>64</sup> NCTC Guidelines, section VI.E.