(UNCLASSIFIED)
Enhanced Safeguards Decision Matrix

Background

The DNI, D/NCTC and the Attorney General approved revised Attorney General Guidelines for NCTC's handling of US Person (USP) information in March 2012. These revised NCTC Attorney General Guidelines ("NCTC's AGGs") govern NCTC's access, retention, use, and dissemination of datasets identified as including non-terrorism information and information pertaining exclusively to domestic terrorism, and provide NCTC with the authority to retain USP information for up to five years (unless a shorter period is required by law, executive order, regulation, international agreement, etc.). During this temporary retention and assessment period, additional safeguards and protections are applied to this data, to include baseline (and potentially enhanced) safeguards, as well as additional compliance, auditing, reporting and oversight mechanisms.

Baseline Safeguards

Pursuant to the 2012 NCTC Attorney General Guidelines, once NCTC secures a new dataset or renegotiates an existing agreement to allow retention of a dataset for a longer period of time, NCTC will, per §III.C.3.d, apply the following Baseline Safeguards to the data:

> *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.*
>
> *(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.

Enhanced Safeguards Assessment

Pursuant to Section III.C.3(e) of NCTC's AGGs, the Director of NCTC, in consultation with the ODNI Office of General Counsel (OGC) and ODNI Civil Liberties Protection Office (CLPO), is required to make a written determination for each dataset as to "whether enhanced safeguards, procedures, and oversight mechanisms are needed."

The Enhanced Safeguards Decision Matrix, reflected below, is designed to aid NCTC in making recommendations to the Director as to whether or not enhanced safeguards may be appropriate for an individual dataset. Each dataset reviewed in this matrix is assessed based upon the fields contained within, and recommendations are tailored to take into account the unique characteristics and needs of each individual dataset. At the same time, one of the underlying goals of this matrix is to facilitate – to the maximum extent possible - consistent treatment of similar datasets with similar sensitivities, and to provide a holistic view of all of the data that NCTC is considering bringing in for Track 3 access under NCTC's revised AGGs.

When deciding if enhanced safeguards are necessary for a given dataset, NCTC is directed to consider a number of factors, including: the sensitivity of the data, the purposes for which the data was originally collected, the means by which the information was acquired, further additional restrictions as agreed to between NCTC and the data provider, the terms of any applicable international agreement regarding the data, the potential harm or embarrassment to a USP that might result from improper use or disclosure of the data, and other relevant considerations. Such considerations are reflected on the horizontal axis in the below Enhanced Safeguards Decision Matrix and are labeled as Columns A – H.

The enhanced safeguards that may be appropriate for a given dataset are reflected on the vertical axis of the Enhanced Safeguards Decision Matrix and are numbered as enhanced safeguards 1 through 10. As depicted, such enhanced safeguards may, for example, require a more restricted user group, special training before data access may be granted, and more frequent reviews to consider whether there is a continued need to retain the dataset given the civil liberties and privacy concerns related to data retention. Enhanced Safeguard 10 is listed as "other" and allows for the crafting of individualized enhanced safeguard deemed necessary and appropriate for addressing the unique sensitivities that may exist in a given dataset.

For purposes of reading this matrix, Y (Yes) and N (No) is used to indicate which specific safeguards are deemed most appropriate to address which particular sensitivities. Likewise, the term "TBD" is incorporated to allow for the crafting of individualized protections customized to the unique sensitivities presented by an individual dataset, and/or customized based upon specific request of the data provider.

For example, if the purpose for which the data was originally collected is "significantly different" from the purpose for which it is now to be used (i.e., national security purposes) – i.e., Column A - then the recommended Enhanced Safeguard protection to address this sensitivity is more frequent reviews of the continued need to retain the dataset, given the civil liberties and privacy concerns related to NCTC's access to the dataset (indicated by a "Y" in box number 6, and "N"s/TBD in the other box numbers under column A).

In reading this matrix, however, the important point to keep in mind is that there are no minimum or maximum number of safeguards that are required to be chosen for a given dataset, as this matrix is meant to be one tool in NCTC's overall, particularized review of each dataset; in other words, the fact that a given safeguard has an "N" listed under a given column, should not be deemed to foreclose the possibility that that safeguard might be warranted in order to address a sensitivity relating to a particular dataset. Likewise, it is possible for a single safeguard to be selected for more than one data sensitivity (as identified on the top axis of the matrix); in other words, just because additional spot checks on dissemination are applied for column A, this would not foreclose their application/use under other columns as well.

Of course, it is understood that the information set forth below is merely a synopsis of all of the relevant and available information on a given dataset, summarized for ease of reference. The below matrix is not intended to be an exhaustive/all-inclusive list of all variables considered, as this matrix is not meant to substitute for individualized discussion and consideration during the in-person Data Acquisition User Group (DAUG) meeting, at which the below summaries will be reviewed.

Comments Specific to Columns A, B and F in the Below Matrix

Column A; Comment 1: *Purpose significantly differs from that for which the data was originally collected*

In assessing whether NCTC's purpose for accessing data under Track 3 differs significantly from that for which it was originally collected, we have consulted available materials relating to disclosures made to individuals at the time the information was collected, including the Routine Uses disclosure contained within applicable System of Records Notices (SORNs), and Privacy Impact Assessments (PIAs) for each of the underlying datasets. To the extent that at least one purpose for the original collection of the data related to counterterrorism (CT) or national security, NCTC will assess such purpose to be consistent with NCTC's purpose for accessing and using the data under Track 3 of the AGGs.

Column B; Comment 2: Sensitivity of the Data

In accordance with OMB Memo M-07-16 (2007), NCTC recognizes that Personally Identifiable Information (PII) includes, but is not limited to, social security numbers, passport numbers, dates of birth, biometrics and other information that "alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual," can be used to identify an individual, and that this data is to be accorded appropriate protection in terms of use, handling and disclosure. To ensure that this PII is appropriately handled, NCTC requires all employees to complete annual Privacy Act/PII training, as well as to comply with NCTC policies specifically related to the handling of PII. In addition to this PII-specific training, the AGG's accord additional protections to all Track 3 ingested datasets – including the PII contained within – through the implementation of baseline safeguards, which include access controls, query restrictions, regular audit and compliance checks, etc. Accordingly, for purposes of determining whether enhanced safeguards are appropriate for a given dataset, the presence of PII is not – in itself - assessed to require safeguards beyond the extensive baseline safeguards already implemented for all datasets. Rather, in assessing the need for enhanced safeguards, NCTC will consider whether the dataset has unique types of especially sensitive PII that warrant additional protection over and above the baseline safeguards and the standard protections employed by NCTC for all PII.

Column F; Comment 3: *NCTC assigned relative risk value related to potential for embarrassment or harm to a USP from improper use/disclosure of the data*

In assessing a dataset for its potential to cause harm or embarrassment to a US Person should improper use or disclosure occur, NCTC recognizes that such a risk is inherent in any system and any dataset, regardless of how remote. In recognition of this fact, NCTC has assigned a relative risk value to this category, ranking risk on a scale of Low/Moderate/High. If a dataset under this category of consideration is deemed to pose a low (or remote) risk of embarrassment or harm from improper use/disclosure, the recommendation is that no enhanced safeguards under this category be imposed for that

dataset. Conversely, should a dataset be deemed to pose a high risk of embarrassment or harm from improper use/disclosure, the recommendation will be for enhanced safeguards to be imposed on that dataset in the hopes of mitigating such risk. Should a dataset fall into the moderate risk category, for example, an asylee already in the U.S., NCTC will attempt to gather additional facts about such risk, to include experiential data from the data provider, in assessing whether or not enhanced safeguards are warranted for that dataset.

Column H; Comment 4: *Type of Query*

Column H is designed to ensure that due consideration is given when a dataset is to be queried in a way that gives rise to unique civil liberty and privacy sensitivities. For example, although NCTC does not currently (as of October 2013) engage in pattern based data mining (as defined in the Federal Agency Data Mining Reporting Act of 2007), NCTC's 2012 Attorney General Guidelines do authorize such activity. Given that data mining implicates a number of unique civil liberty and privacy concerns, including potential high false positive rates, Column H ensures that these concerns are considered and addressed by NCTC when determining if Enhanced Safeguards are appropriate.

Enhanced Safeguards Decision Matrix

SENSITIVITIES									
SAFEGU		**A. Purpose significantly differs from that for which data originally collected (Note: See Comment 1)**	**B. Sensitivity of the Data (Note: See Comment 2)**	**C. The means by which the information was acquired**	**D. Operational sensitivities implicated by the data (e.g., sources and methods)**	**E. Enhanced Safeguards/ Protections mandated by International Agreement**	**F. NCTC assigned relative risk value related to potential for embarrassment or harm to a USP from improper use/disclosure of the data (Note: See Comment 3)**	**G. Data Provider required safeguards**	**H. Type of query (Note: See Comment 4)**
	1. Access to the datasets limited to a more restricted user group, based on roles determined in coordination with the data provider	N	Y	N	Y	TBD by agreement	N	TBD by agreement	Y
	2. Coordination with the data provider and legal required prior to any dissemination of non-terrorism information derived from the dataset (even for disseminations explicitly authorized in the Guidelines themselves)	N	N	Y	Y	TBD by agreement	Y	TBD by agreement	Y
	3. Access to the dataset contingent upon completing special training regarding use and handling of the specific data	N	Y	N	Y	TBD by agreement	Y	TBD by agreement	N
	4. After _[1] years from the date of receipt of the data, the data will no longer be included in automated correlation results. Searches must be pre-approved by an NCTC Official at the Group Chief or higher level	N	N	N	N	TBD by agreement	N	TBD by agreement	Y

[1] An explicit period of time shall be recommended in place of this blank, based upon the DAUG's individualized assessment of a given dataset.

Enhanced Safeguards Decision Matrix

A R D S	5. After [2] years from the date of receipt of the data, NCTC shall employ privacy enhancing technologies/techniques that allow USP information or other sensitive information to be "discovered" without providing the content of the information, until the appropriate standard is met	N	Y	Y	N	TBD by agreement	N	TBD by agreement	Y
	6. More frequent reviews (every __[3] months) of the continued need to retain the dataset given the civil liberties and privacy concerns related to retention of the data	Y	N	N	N	TBD by agreement	N	TBD by agreement	Y
	7. Additional spot checks (no less frequently than ___[4]) to verify compliance with the enhanced access restrictions (See 1, above)	N	Y	N	Y	TBD by agreement	N	TBD by agreement	Y
	8. Additional spot checks (no less frequently than ___[5]) to verify compliance with pre-dissemination coordination requirement (See 2, above)	N	N	Y	Y	TBD by agreement	Y	TBD by agreement	Y
	9. Additional spot checks (no less frequently than ___[6]) to ensure that no other searches of the dataset, other than those authorized pursuant to 4 (above), have been conducted during the previous period	N	N	N	N	TBD by agreement	N	TBD by agreement	Y
	10. Other.	TBD	TBD	TBD	TBD	TBD by agreement	TBD	TBD by agreement	TBD

[2] An explicit period of time shall be recommended in place of this blank, based upon the DAUG's individualized assessment of a given dataset.
[3] An explicit period of time shall be recommended in place of this blank, based upon the DAUG's individualized assessment of a given dataset.
[4] An explicit period of time shall be recommended in place of this blank, based upon the DAUG's individualized assessment of a given dataset.
[5] An explicit period of time shall be recommended in place of this blank, based upon the DAUG's individualized assessment of a given dataset.
[6] An explicit period of time shall be recommended in place of this blank, based upon the DAUG's individualized assessment of a given dataset.