[redacted]

[Downgrade to UNCLASSIFIED//FOUO when separated from classified annex]

(U) National Counterterrorism Center

Attorney General Guidelines For Access, Retention, Use And Dissemination By The National Counterterrorism Center And Other Agencies Of Information In Datasets Containing Non-Terrorism Information

(U) Annual Report on the Access, Retention, Use and Dissemination of United States Person Information

For the Period March 23, 2012 through March 31, 2013

[redacted]

(U) Director, National Counterterrorism Center
Annual Report on the Access, Retention, Use and Dissemination of United States Person Information
March 23, 2012 through March 31, 2013

I. Introduction

(U) The Director, National Counterterrorism Center, provides this report pursuant to §VI.D.2 of the 2012 NCTC Attorney General Guidelines (AGGs), entitled *Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information.*

A. Scope

(U) This report covers the activities of the National Counterterrorism Center from March 23, 2012 through March 31, 2013 (hereinafter "the reporting period").[1]

(U) As of the end of the reporting period, NCTC had not yet executed any Terms and Conditions (T&Cs) under the 2012 NCTC AGGs. As such, all Track 3 datasets replicated at NCTC were still being accessed under NCTC's 2008 AGGs, which require application of a "promptly review" and remove standard for review of US persons information.

(U) Nonetheless, because the annual reporting requirement applies to NCTC's access of data through all three tracks of access – including Tracks 1 (account-based access on a data provider's native system) and 2 (queries provided to a data provider for the data provider to run on its own systems) - NCTC deems the annual reporting requirement to already be in effect. NCTC is therefore submitting this report in accordance with the 2012 NCTC AGGs reporting requirement.

B. Reporting Requirement

(U) Section VI.D.2 of the 2012 NCTC AGGs requires that 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*."

(U) Furthermore, §VI.D.3 of the 2012 NCTC AGGs requires that the "*NCTC shall provide a copy of this report to the ODNI General Counsel and the IC Inspector General, and shall make*

[1] (U) The 2012 NCTC AGGSs state only that the Director of NCTC "shall report annually in writing," but does not specify the date in which the reporting should begin nor the time period to be covered in the initial report. As such, this first annual report will cover the period from March 23, 2012, the day after the 2012 NCTC AGGSs were signed, through 31 March 2013. Hereafter, all subsequent annual reporting periods will run from April 1st of one year to March 31st of the following year (e.g., the next annual report will cover the period of April 1, 2013 through March 31, 2014).

the report available upon request to the Assistant Attorney General for National Security."

C. Report Content

(U) Pursuant to §§VI.D.2(1) through VI.D.2(9) of the 2012 NCTC AGGs, Part II of this report addresses each of the nine areas on which NCTC is required to report annually.

D. Protection of Privacy and Civil Liberties

(U) Privacy and civil liberties protection at NCTC is accomplished through an array of compliance and oversight mechanisms. For example, NCTC activities receive review and oversight from the ODNI Civil Liberties Protection Officer, who leads the ODNI's Civil Liberties and Privacy Office (CLPO), and who has statutorily defined duties under the National Security Act of 1947 and the Intelligence Reform and Terrorism Prevention Act of 2004. In addition, NCTC has a full-time on-site Civil Liberties and Privacy Officer (NCTC CLPO), who reports directly to the ODNI Civil Liberties Protection Officer. As detailed more fully in this report, over the past year, the NCTC CLPO has worked closely with the NCTC Office of Legal Counsel ("NCTC Legal") to oversee implementation of the 2012 NCTC AGGs, ensuring appropriate legal, privacy, and civil liberties safeguards are incorporated into the policies, processes and procedures that implement and support NCTC's access to and use of data under the 2012 NCTC AGGs.

(U) NCTC's activities are also subject to review and oversight by the ODNI Office of General Counsel (OGC) and the IC Inspector General. The Department of Justice is also consulted on issues relating to the AG Guidelines, and receives a report if there are "significant failures" in handling of data covered by the 2012 NCTC AGGs. In addition, as required by applicable executive orders, NCTC is required to report violations of law and executive order to the Intelligence Oversight Board of the President's Intelligence Advisory Board. NCTC must also keep the intelligence oversight committees in Congress fully and currently informed of its activities, and must report legal violations to them. Finally, NCTC is also subject to the oversight of the Privacy and Civil Liberties Oversight Board (PCLOB).

II. Nine Mandated Areas to be Included in Annual Report

(U) The nine mandated areas for inclusion in the annual report[2] and NCTC's response to each are as follows:

A. (U) **Periodic Reviews:**[3] Pursuant to Section VI.B of the 2012 NCTC AGGs, NCTC, in coordination with the ODNI Civil Liberties Protection Officer, is required to conduct periodic reviews of all datasets replicated under Track 3 to determine whether retention and continued assessment of the United States person (US person) information in those datasets remains appropriate.[4] In addition, NCTC must also conduct periodic reviews of the continued

[2] (U) 2012 NCTC AGGSs, §§VI.D.2(1) through VI.D.2(9)
[3] (U) Id., §VI.D.2(1)
[4] (U) In conducting this review, consideration shall be given to: (1) The purpose for which the dataset was acquired; (2) the success of that dataset in fulfilling legitimate counterterrorism purposes' (3) a determination regarding whether those purposes can now be fulfilled through Track 1 or 2 access to the dataset, through the use of other

necessity and efficacy of bulk disseminations permitted under the Guidelines. Lastly, NCTC must report the results of both types of periodic reviews to the IC Inspector General.

(U) As of the end of the reporting period, NCTC was still working with its data providers to finalize the Terms and Conditions required by the 2012 NCTC AGGs. As such, the periodic review of Track 3 datasets requirement was deemed to have not yet been triggered during the reporting period. Once NCTC has executed new T&Cs that incorporate the requirements of the 2012 NCTC AGGs, however, NCTC will work with the NCTC CLPO and an NCTC-wide governance board responsible for the management and prioritization of data access, acquisition, and retention to conduct, on at least an annual basis,[5] a review of all Track 3 datasets to determine the appropriateness of continued retention of the US person information and the adequacy and effectiveness of the safeguards applied.

(U) Similarly, as of the end of the reporting period, NCTC was not conducting bulk disseminations and thus the required reviews to examine the continued necessity and efficacy of bulk disseminations were not applicable. Should NCTC choose at some future point in time to consider engaging in bulk dissemination (as permitted under Sections IV (B) and (C) of the 2012 NCTC AGGs), NCTC will evaluate, on a case by case basis, the appropriateness of such request, and will report on such activities (if any are authorized as of the relevant reporting period) in Section II(F) of subsequent annual reports.

B. (U) ***A general description of NCTC's compliance and audit processes;***[6]

(U) During the temporary retention period, the 2012 NCTC AGGs require that four specified baseline safeguards be applied to all datasets acquired pursuant to Track 3. Below is a brief discussion of each of the four baseline safeguards and the audit and compliance processes that NCTC has developed to ensure successful implementation of these requirements. Additional detail can be found at Attachment 1.[7]

(U) **Baseline Safeguard 1**:

(U) *"These datasets will be maintained in a secure, restricted-access repository."*[8]

(U) For Baseline Safeguard 1, NCTC will focus on privileged users who have system administrator-like access to the secure, restricted access repositories where all Track 3 datasets are maintained. In addition to training these privileged users on appropriate access to, and use of, the Track 3 datasets, NCTC will audit the repositories, on a quarterly basis, to ensure that only privileged users accessed the repositories and that the user's accesses within each repository was limited to those datasets for which he/she was authorized. To verify that

---

datasets in NCTC's possession, or through other appropriate means, and; (4) privacy and civil liberties considerations applicable to the particular dataset.

[5] (U) More frequent reviews may be required, as an Enhanced Safeguard, when deemed appropriate for an individual dataset.

[6] (U) 2012 NCTC AGGSs, §VI.D.2(2)

[7] (U) Attachment 1 details each of the four baseline safeguards, and the specific processes and procedures that NCTC will utilize to monitor compliance.

[8] (U) 2012 NCTC AGGSs, §III.C.3.d(1)

only approved users had access to each repository and that the user only accessed Track 3 datasets for which they were authorized, up to [redacted] randomly selected accesses from [redacted] percent of all Track 3 data locations in both repositories (includes physical serves and databases) in a twenty four hour period will be evaluated. As discussed above, however, as of the end of the reporting period NCTC had not yet replicated any datasets under Track 3 of the 2012 NCTC AGGs. Therefore, as of the end of the reporting period, NCTC has not yet begun the audit checks described above for Baseline Safeguard 1.

(U) **Baseline Safeguard 2**:

(U) *"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."*[9]

(U) Baseline Safeguard 2 is implemented through NCTC's role-based access policy. More specifically, role based access to datasets within NCTC is restricted by membership in pre-approved virtual groups (generally, broken out by offices within an individual NCTC Directorate) and is contingent upon adherence to NCTC's information sharing and use rules, the appropriate security clearance, the need to know in the course of official duties and completion of required training. In addition, annual training on data access and use, privacy, and U.S. persons is required along with dataset specific training, as appropriate. Training is required prior to data access and those who fail to complete their annual training will lose access to the data.

(U) In order to verify appropriate implementation of and continued compliance with the role-based access requirement, spot checks will be conducted every quarter to ensure that all members in pre-approved groups – which is the basis for access to a particular dataset - are accurate and up to date, and thus continued access to the particular Track 3 dataset is appropriate. Conversely, once an employee physically moves to a new office, that employee's accesses to datasets are reassessed and updated (as needed), based upon mission need within the new assignment.

(U) Spot checks are performed using the pre-approved group member list for the chosen audit date. The Reviewer will compare the pre-approved group member list against an up to date office staffing list for that same date. If all members of the pre-approved group are still employed in the corresponding office group on the chosen date, then the Reviewer will have verified role-based access for that group. If on the other hand, an individual listed in the pre-approved group has since left the office responsible for the pre-approved group member list (for example, the employee moved to a new office), then the Reviewer will further check to see whether the individual in question gained access to a dataset using the outdated group membership, and if so, whether the employee was authorized to access that dataset in his/her new role (i.e., if the employee's new group is also authorized to access the same dataset, then there has been no unauthorized access to the dataset, even though the group membership list will need to be updated to reflect the employee's updated assignment going forward).

[9] (U) 2012 NCTC AGGSs, §III.C.3.d(2)

[redacted]

(U) Although NCTC has not yet completed any T&Cs subject to the 2012 NCTC AGGs, NCTC has trained all personnel in accordance with section III.B.3 of the AGGs, including all new personnel who are trained as part of NCTC's orientation process.

(U) **Baseline Safeguard 3**:

(U) *"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."*[10]

(U) NCTC defines "logons" as any access to a Track 3 dataset via an application accessible to an NCTC user. NCTC monitors, records, and audits logons to all Track 3 datasets and will verify compliance with the Safeguard by sampling, on a quarterly basis, all logons to all Track 3 datasets to ensure that the logons were authorized. Logons to a dataset will be presumed authorized after the appropriate manager from the Directorate or office confirms that the user was assigned to his/her organization on the date chosen for review and that access to that Track 3 dataset was appropriate. NCTC will do this by reviewing logon activity against the role-based accesses controls established under Baseline Safeguard 2 to ensure the logons were consistent with the user's role. Logoffs will not be independently tracked as the ending of a query or set of queries on a dataset will constitute a "logoff" from the dataset.

(U) NCTC will also monitor, record, and audit changes and manipulations to all Track 3 dataset files/objects to identify any unauthorized file/object changes or manipulations. File/object changes and manipulations can only be made by NCTC privileged users. No application accessible to an NCTC user is capable of making file changes or manipulations. Because file/object changes and manipulations of data are a regular part of the processes required to extract, transform, and load data to make it available within applications and tools, NCTC's process needs to differentiate authorized changes/manipulations from those that are unauthorized. To do this, on a quarterly basis, NCTC will randomly select [redacted] percent of all Track 3 servers for audit and will query its audit log tool for specified fields which indicate that a change and/or manipulation has occurred. A script will then be run to select [redacted] percent, but not more than [redacted], changes/manipulations per server. To verify that each change/manipulation was authorized, Mission Systems will provide a record of each change/manipulation made to the supervisor of the individual who performed the change/manipulation. The supervisor will then review the change/manipulation, determine if the change/manipulation was authorized and report their findings to Mission Systems.

(U) Queries executed will be monitored, recorded, and audited using NCTC's procedures which implement Baseline Safeguard 4, described below.

[10] (U) 2012 NCTC AGGSs, §III.C.3.d(3)

[redacted]

(U) NCTC will also review, on a quarterly basis, a sampling of the audit records captured for all accesses to, and manipulations of, Track 3 datasets to verify and document that there were no unauthorized accesses, modifications, or deletions made to those audit records. All audit records will be retained in accordance with the Federal Records Act, NCTC's applicable records control schedules, and Intelligence Community Standards, and for no less than two years to ensure NCTC can meet its obligations under the Attorney General Guidelines.

(U) As discussed above, however, as of the end of the reporting period NCTC had not yet replicated any datasets under Track 3 of the 2012 NCTC AGGs. Therefore, NCTC has not yet begun the audit checks described above for Baseline Safeguard 3.

(U) **Baseline Safeguard 4**:

(U) *"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. (emphasis added)"*[11]

(U) To ensure that queries against Track 3 datasets are narrowly tailored in accordance with the query design requirements of the 2012 NCTC AGGs, query reviews will be conducted once every quarter by selecting queries run during a one month period within that quarter. Query reviews will be conducted by Branch Chiefs from all branches that use Track 3 data. Prior to conducting query reviews, Branch Chiefs will first attend mandatory Branch Chief Query Review Training to ensure both a clear understanding of the 2012 NCTC AGGs and the resultant requirements set forth in those Guidelines with regard to querying that data.[12]

(U) Once the designated audit month within the respective quarter has been chosen, Mission Systems will implement a process by which all queries run on Track 3 datasets during that month will be identified for each respective branch, randomized, and populated into a user interface for review. The file for each branch is "shuffled" using a shuffling algorithm, a custom code and industry standard way to randomize data in a software language.[13]
(U) Initially, [redacted] randomly selected queries will be produced for each branch during the chosen month being audited (or a lesser number if a branch did not conduct [redacted] or more queries). The number of queries reviewed may increase based upon lessons learned from one quarter to the next.

[11] (U) 2012 NCTC AGGSs, §III.C.3.d(4)
[12] (U) Attachment 3, Criteria/Guidance for Conducting Query Reviews
[13] (U) The Ruby data randomization used in selecting queries for review is analogous to selecting names from a hat. Once the name is removed from the hat, it cannot be placed back into the hat to be selected again. Therefore, the original number of available names is reduced by one and another random selection takes place. The selected names are placed in the order they were selected until all of the names are removed from the hat.

(U) To facilitate and automate the query review process, Mission Systems has created a SharePoint site to serve as a user interface that will be populated with each Branch's randomly selected queries. The Branch Chief Query Review Training will include a demonstration of the SharePoint site as the Branch Chief will both review and adjudicate the query within the SharePoint.

(U) Each query reviewed will be assessed by the Branch Chief to ensure that the query is designed solely to identify information that is reasonably believed to constitute terrorism information while minimizing the review of information concerning US persons that does not constitute terrorism information. All non-compliant queries will be reported to NCTC CLPO and Legal, as well as the NCTC Front Office. As an additional protection, Branch Chiefs will not be permitted to review their own queries. Should a Branch Chief's query come up as one of the [redacted] randomly selected queries for review in a given branch, a process has been implemented to ensure that this Branch Chief's query is reviewed by another Branch Chief for purposes of compliance validation.

(U) The NCTC CLPO and the NCTC Office of Legal Counsel will provide oversight of NCTC's compliance with these safeguards, spot checks and other audit mechanisms, to include reviewing the results of the spot checks and audits conducted by NCTC for Baseline Safeguards 1-4.

C. (U) ***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;***[14]

(U) Please refer to paragraph II.B above. While NCTC has already developed and tested processes/procedures necessary to assess and ensure compliance with all four of the Baseline Safeguards reflected in the Guidelines, there are not yet any results to report because, as of the end of the reporting period, Track 3 replication has not yet been implemented under the 2012 NCTC AGGs.

D. (U) ***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;***[15]

(U) While no data has been received under the 2012 NCTC AGGs as of the end of the reporting period, NCTC plans to use the same tools and automated processes now in place under the 2008 AGGs for tracking and deleting non-terrorism US person information under the 2012 NCTC AG Guidelines. All NCTC personnel are trained regarding access to non-terrorism datasets and USP information under the 2012 AGGs. Such training includes instruction that any terrorism information identified via Tracks 1 or 2 that is subsequently determined not to constitute terrorism information must be purged from NCTC's systems.

[14] (U) 2012 NCTC AGGSs, §VI.D.2(3)
[15] (U) Id., §VI.D.2(4)

(U) To ensure compliance with the requisite deletion rules, the NCTC Data Management Team (DMT)[16] uses the Data Catalog[17] along with Excel spreadsheets to track and monitor planned and actual data deletion dates. To ensure Center compliance, the DMT sends a broadcast email on a weekly basis to all entities within the Center who have access to data with near-term deletion dates. The email notifications begin four weeks prior to the scheduled deletion date, and occurs on a weekly basis thereafter, to ensure that the entity is aware and mindful of the imminent and upcoming deletion date and can plan accordingly.

(U) All Center entities that access and/or hold data perform data deletions using standard operating procedures (SOPs) in accordance with their respective business processes. DMT is responsible for scheduling all data deletions and notifying responsible parties of impending deletions. Within MS, the Data Factory[18] is responsible for logging all data deletions into a central database. Both DMT and Data Factory will use this database, in addition to audits and spot checks, to verify that required deletions occurred as planned.

~~(U//FOUO)~~ During the reporting period, it was recommended that NCTC's Track 3 deletion process (under the 2008 Guidelines) be changed so that deletions are scheduled to occur a number of days before the end of the authorized retention period (as opposed to on the last day), to ensure that if for any reason a deletion fails to occur as planned, it can be detected and remedied before the retention period has expired. Specifically, Mission Systems has recommended that NCTC approve establishing a planned deletion date of seven days prior to the required deletion date for all data in NCTC's holdings[19]. The current deletion practice entails setting the planned deletion date on the last day of the retention period, thereby providing no margin for error should problems occur, or mistakes be made, at the time of deletion. While understandable that the Center would want to retain the data for as long as is permissible in the event the information could be useful in supporting terrorism analysis, such a practice allows for no flexibility and a deletion delay of any length may result in a compliance incident.

E. (U) *An assessment of United States person information disseminated by NCTC directly to foreign, international, state, local, tribal, or private sector entities or individuals; the*

[16] (U) The Data Management Team (DMT) is a group in NCTC Mission Systems that receives/accepts data from NCTC mission partners (i.e., data providers). Using the retention parameters specified in the Memorandum of Understanding between NCTC and the data provider, DMT calculates a deletion date for each delivery of each dataset and posts both the receipt and deletion dates in the Data Catalog.

[17] (U) The Data Catalog is a centralized service used to manage information about datasets held by NCTC. The primary purpose of this application is to track, organize, and publish information about datasets relating to NCTC's mission and authorities.

[18] ~~(U//FOUO)~~ The Data Factory is the organization within NCTC Mission Systems that is responsible for the replicating of all data received from data providers into the NCTC Counter Terrorism Data Layer (CTDL). After replicating the data into the CTDL, the Data Factory then indexes the data and exposes it, through the use of various tools, so that the data may be used by analysts. Prior to exposing the data, the Data Factory uses the authoritative deletion dates entered into the Data Catalog by DMT to mark every record replicated with its appropriate deletion date. In addition, the Data Factory deletion process queries each record of each dataset daily to determine whether its deletion date has been reached. If the record does not carry a "Hold," which indicates there is an exigent threat requiring the data not be deleted prior to the deletion date, or "Terrorism Information" flag and the deletion date is within seven days, the record is deleted and the deletion is then recorded in the deletion logging database.

[19] (U) In April of 2013 this recommendation will be considered by an NCTC-wide governance board responsible for the management and prioritization of data access, acquisition, and retention.

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;[20]

(U) As of the end of the reporting period, NCTC had not disseminated US person information directly to foreign, international, state, local, tribal, or private sector entities or individuals under the 2012 NCTC AGGs. Should this occur in the future, NCTC has a process to identify and tag all such data so that the dissemination can be tracked and reported in future annual reports.

F. (U) ***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;***[21]

(U) As of the end of the reporting period, there were no accesses to, or disseminations of, bulk datasets or significant portions of datasets.

(U) Should NCTC choose at some future point in time to consider engaging in bulk dissemination (as permitted under Sections IV(B) and (C) of the 2012 NCTC AGGs), NCTC will evaluate, on a case by case basis, the appropriateness of such request, and will report on such activities (if any are approved) in subsequent annual reports.

G. (U) ***As 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;***[22]

(U) Enhanced Safeguards Assessment: Pursuant to Section III.C.3(e) of the 2012 NCTC AGGs, the Director of NCTC, in consultation with the ODNI General Counsel and ODNI Civil Liberties Protection Officer, is required to review each dataset subject to the 2012 NCTC AGGs and make a written determination as to "whether enhanced safeguards, procedures, and oversight mechanisms are needed" prior to replication. In making this assessment, NCTC is directed to consider a number of factors, including: the sensitivity of the data, the purpose(s) for which the data was originally collected, 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, the terms of any applicable international agreement regarding the data, the potential harm or embarrassment to a US person that might result from improper use or disclosure of the data, and other relevant considerations.

(U) Because the Enhanced Safeguards assessment requirement did not exist under the 2008 AGGs, NCTC has undertaken to assess each Track 3 dataset anew for application of

[20] (U) Id., §VI.D.2(5)
[21] (U) Id., §VI.D.2(6)
[22] (U) Id., §VI.D.2(7)

Enhanced Safeguards prior to signing new T&C documents for datasets under the 2012 NCTC AGGs. Specifically, NCTC has an internal process wherein an NCTC-wide governance board responsible for the management and prioritization of data access, acquisition, and retention initially reviews each Track 3 dataset and then makes recommendations to the D/NCTC regarding the appropriateness of enhanced safeguards.

(U) To aid this board, a Track 3 Enhanced Safeguards Matrix (Attachment 2) has been developed. This matrix is only one of the tools used by NCTC in its particularized review of each dataset, and is meant to serve only as a starting point for the board as it considers whether, and which, enhanced safeguards may be appropriate. Each dataset is reviewed against the matrix and recommendations are tailored to take into account the unique characteristics and sensitivities 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 2012 AGGs.

(U) As of the end of the reporting period, the board had reviewed and made recommendations specific to [redacted] Track 3 datasets, which were being coordinated with both the ODNI General Counsel and the ODNI Civil Liberties Protection Officer. Upon completion, all information will be forwarded to the D/NCTC for review and decision.

H. (U) ***A description of measures that NCTC has taken to comply with the requirements of section VI.C[23] with respect to its data processing systems;[24]***

(U) As detailed throughout this report, numerous efforts were undertaken during the reporting period to enhance NCTC's ability to monitor activity involving US person information and other sensitive information, while facilitating compliance with, and the auditing and reporting required by, the 2012 NCTC AGGs. Such activities include, but are not limited to, the following:

- (U) Verified and validated the capture (logging) of all activity, both by privileged users (system administrators) and end users, involving US persons Track 3 data. Enhanced the detail of the information captured in the logs and closed any logging gaps discovered;
- (U) Auditing a random sampling of all accesses to US persons data to monitor and verify that the user was authorized to access the data and did so in compliance with the requirements specific to that dataset;
- (U) Display informational banners within the tools utilized to access Track 3 datasets to remind users that they are about to search on a Track 3 dataset and, as such, that their query must be designed in accordance with 2012 NCTC AGG requirements;

[23] (U) Id., Section VI.C, NCTC's Computer Systems, reads as follows**:** 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.
[24] (U) Id., §VI.D.2(8)

- (U) Established a SharePoint site to facilitate and automate the review of selected queries to ensure that query design is in compliance with 2012 NCTC AGG requirements;
- (U) Training conducted at all levels to ensure personnel understand the 2012 NCTC AGGs and their role/responsibilities in upholding and complying with them.

I. (U) ***A description of any material changes or improvements NCTC implemented, or is considering implementing, to improve compliance with these Guidelines;***[25]

(U) Material changes and improvements have occurred within the Center throughout the reporting period which has had an immediate and positive impact on NCTC monitoring and compliance activities in support of the 2012 NCTC AGGs. To facilitate both awareness of, and compliance with, deletion requirements specific to US persons, a "US Person Planned Deletion Date" field was added to the Data Catalog in August of 2012 so that the Catalog now specifies the planned deletion date for both US person and non-US person information. In addition, deletion scripts have been automated to eliminate the need for human intervention and thus minimize the potential for human error.

~~(U//FOUO)~~ Mission Systems has recommended that NCTC approve establishing a planned deletion date of seven days prior to the required deletion date for all data in NCTC's holdings as the existing practice of setting a planned deletion date on the final date by which a record is required to be removed allows for no flexibility should even a simple delay in the deletion process occur (for example, if the deletion delay is not discovered until the following day after the required deletion date).

(U) Deletion verification has also been improved. Rather than relying solely on conducting periodic and random spot checks to ensure that a deletion script has launched, NCTC now also conducts post-deletion validation for all planned deletions to verify not only the launching of the deletion script, but also that the deletion did, in fact, occur as scheduled.

(U) In addition to automating the deletion scripts, significant improvements have been made in the tailoring of the deletion scripts. At the beginning of the reporting period, deletion scripts were written to be specific to an identifier established by the data provider for each record. After recognizing that a data provider may use the same identifier when referring to two different collections (i.e. duplicate identifiers in different datasets), NCTC customized all deletion scripts to be collection specific (i.e. the script is tailored specifically for that dataset), thus mitigating the possibility of duplicate identifiers in different datasets.

~~(U//FOUO)~~ NCTC is also in the process of implementing modifications to a web based tool to establish a 'dashboard' to reflect the ongoing status of various hosts and services related to deletions. The dashboard will also be capable of sending notifications to appropriate personnel when it detects a problem in the area for which the individual is responsible.

(U) To facilitate and improve transparency and collaboration, the process for reporting and

[25] (U) Id., §VI.D.2(9)

addressing compliance incidents was also revamped during the current reporting period. The reporting review template utilized by the Center to report a compliance incident has been refined to be more fact-specific in identifying both the cause of the incident as well as remediation measures that will be put in place to prevent reoccurrence. In addition, NCTC CLPO, NCTC Legal and the Information Sharing Program and Policy Office (ISPPO) have worked together to develop and improve both the transparency with which reporting occurs and the sharing and collaboration between the three offices in the handling and adjudication of compliance incidents. More specifically, a shared template has been developed for use by the Center to outline the facts, timeline, reporting requirements and remediation measures for each compliance incident. In addition, NCTC issued Compliance Incident Procedures Regarding Data Handling during the reporting period, which sets forth for the Center requirements for reporting, assessing, investigating and resolving compliance incidents, updating and expanding on the interim guidance under which NCTC had previously been operating. Finally, to ensure easy access to compliance materials and lessons learned for the sharing and education of the Center as a whole, a repository and tracking system has also been created for use by those NCTC entities with compliance responsibilities.

~~(U//FOUO)~~ Competing mission priorities and shrinking budgets have, however, adversely affected several planned efforts at investigating Privacy Enhancing Technologies. Plans to establish a suitable test environment at NCTC have been delayed. In addition, the planned analysis and evaluation of promising commercial technologies that allow data masking has been postponed. While NCTC had hoped to pursue such efforts during the 2012–2013 reporting period, such efforts were precluded, in part, by the unanticipated costs associated with the planning and implementation of baseline safeguards and the operations and maintenance of Track 3 data replicated pursuant to the 2008 AG Guidelines.[26] In addition, NCTC's terrorist watch listing, counterterrorism analysis, and threat management mission needs continue to focus Mission Systems' limited technology budget to near-term, mission-essential capabilities exclusively, with no latitude at present for establishing an experimental capability.

~~(U//FOUO)~~ In addition to NCTC internal efforts, the Intelligence Advanced Research Projects Activity (IARPA) continues its work on a research program entitled "Security and Privacy Assurance Research".[27] During the last year, NCTC drafted a Memorandum of Understanding that will allow IARPA to assess the performance of their research algorithms against synthetic data that are generated based upon TIDE schema. Technology transition will be greatly streamlined by testing and evaluating IARPA developed capabilities against mission realistic data and operational scenarios.

(U) In addition to the above, a classified annex, containing more detailed information on NCTC efforts associated with research and development, has been prepared and appended to this report.

III. NCTC AG Guidelines Outreach & Transparency Measures

[26] (U) NCTC's Track 3 replication and data handling requirements specify improved baseline safeguards which require capital investment to enhance our current access control system. To minimize mission productivity loss during implementation, Mission Systems has produced an Investment Business Case. The Access Control investment is in the top tier of new acquisition activities planned for FY14.

[27] (U) See *"Office of the Director of National Intelligence 2011 Data Mining Report for the Period January 1, 2011 through December 31, 2011"*, paragraph III.C.3

(U) As part of its commitment to providing appropriate transparency to mission partners, Congress, and the American public, NCTC has undertaken numerous efforts to provide briefings on the 2012 NCTC AGGs, as well as NCTC's progress in implementing these Guidelines. For example, as of the end of the reporting period NCTC had provided multiple briefings on the 2012 NCTC AGGs to its traditional intelligence oversight committees in both the House and Senate, as well as to other Congressional committees that have shown an interest in the Guidelines. NCTC also met on a number of occasions with the Privacy and Civil Liberties Oversight Board (PCLOB) in order to provide them background on NCTC's access, retention, use and deletion of Track 3 US persons data under the 2008 and 2012 NCTC AGGs, as well as NCTC's progress on implementation of the civil liberties and privacy protections required by these 2012 Guidelines.

(U) Cognizant of the importance of earning and retaining the public trust in its mission, NCTC also endeavored during the reporting period to engage in a number of transparency enhancing measures with the public.

(U) For example, NCTC issued a public press release when the revised 2012 NCTC AGGs were first signed, providing detailed information to the public about the primary changes under the revised Guidelines, as well as the additional protections incorporated within those Guidelines. NCTC also subsequently released - and posted on its website - an unclassified version of the Guidelines, along with a Mission Justification Fact sheet explaining the mission reasons behind NCTC's revised Guidelines. As a further transparency measure, the ODNI Civil Liberties and Privacy Office also posted a detailed analysis of the 2012 NCTC AGGs, including the civil liberties and privacy protective measures contained within those Guidelines.

(U) NCTC is planning a number of additional transparency enhancing measures for the next reporting period. We look forward to providing updates on these and other initiatives, in our next annual report.

Attachment:
1. (U) Classified Annex (Document is [redacted])
2. (U) Baseline Safeguards 1-4 (Document is FOUO)
3. (U) Enhanced Safeguards Decision Matrix (Document is FOUO)
4. (U) Criteria/Guidance for Conducting Query Reviews (Document is FOUO)