(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 1 April 2013 through 30 September 2015

(U) Director, National Counterterrorism Center
Annual Report on the Access, Retention, Use and Dissemination of United States Person Information
1 April 2013 through 30 September 2015

A. 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.*

1. Scope

(U) This report, submitted in accordance with the 2012 AGGs reporting requirement, covers the activities of the National Counterterrorism Center from 1 April 2013 through 30 September 2015 (hereinafter "the reporting period") and applies to NCTC's access to data through all three tracks of access – Track 1 (account-based access on a data provider's native system), Track 2 (queries provided to a data provider for the data provider to run on its own systems) and Track 3 (NCTC replication of portions or the entirety of a dataset when necessary to identify the information that constitutes terrorism within the dataset). Note, the preceding annual report covered the period 23 March 2012, the day after the 2012 NCTC AAGs were signed, through 31 March 2013. This report addresses the entire period since the initial report through 30 September 2015. In doing so, NCTC is hereby adjusting the reporting period for future reports to a fiscal year (October 1 – September 30) reporting period.

(U) As of the end of the reporting period, NCTC had executed seven Terms and Conditions (T&Cs) under the 2012 AGGs for ten Track 3 datasets. The agreed upon retention periods were negotiated with the respective data providers and ranged in time from one to five years.

2. Reporting Requirement

(U) Section VI.D.2 of the 2012 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 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 the report available upon request to the Assistant Attorney General for National Security.*"

3. Report Content

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

4. Protection of Privacy and Civil Liberties

(U) NCTC accomplishes privacy and civil liberties protection 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); their duties are statutorily defined duties under the National Security Act of 1947 and the Intelligence Reform and Terrorism Prevention Act of 2004. In addition to the ODNI CLPO, NCTC has a full-time on-site Civil Liberties and Privacy Officer (NCTC CLPO), who reports directly to the ODNI Civil Liberties Protection Officer. Over the past 2.5 years, the NCTC CLPO worked closely and extensively with the NCTC Office of Data Strategy and Innovation (ODSI) Compliance and Transparency Group (hereafter NCTC Compliance) and the NCTC Office of Legal Counsel (NCTC Legal) to oversee implementation of the 2012 AGGs. This collaboration ensured the incorporation of appropriate legal, privacy, and civil liberties safeguards into the policies, processes and procedures, which implement and support NCTC's data access and usage under the 2012 AGGs.

(U) NCTC's data access and usage activities are also subject to review and oversight by the ODNI Office of General Counsel (OGC) and the IC Inspector General (IC IG). Additionally, NCTC consults the Department of Justice (DOJ) on matters involving the AG Guidelines. Upon completion of findings involving dataset access and usage, DOJ receives a report if "significant failures" occur with the handling of data covered by the 2012 guidelines. As required by applicable executive orders and transparency initiatives, NCTC reports violations of law and executive order to the Intelligence Oversight Board (IOB) of the President's Intelligence Advisory Board (PIAB) and Privacy and Civil Liberties Oversight Board (PCLOB). Lastly, NCTC strives to keep Congressional intelligence oversight committees fully abreast of data activities by reporting legal violations in a timely and detailed manner.

B. **Nine Mandated Areas to be included in Annual Report**

(U) The nine mandated areas for inclusion in the annual report[1] and NCTC's response to each are as follows:

1. **(U) Periodic Reviews**

(U) Pursuant to Section VI.B of the 2012 AGGs, NCTC, in coordination with the ODNI Civil Liberties Protection Officer, is required to conduct periodic reviews of all datasets replicated under Track 3[2]. These reviews assist with determining whether retention and continued assessment of the United States person (U.S. Person) information in those datasets remains appropriate.[3] In addition, NCTC conducts periodic reviews of the continued necessity and efficacy of bulk disseminations permitted under the Guidelines. NCTC reports the results of both types of periodic reviews to the IC IG as required by the 2012 AGGs.

[1] (U) 2012 AGGs, §VI.D.2(1) through VI.D.2(9)
[2] (U) Id., §VI.D.2(1)
[3] (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 datasets in NCTC's possession, or through other appropriate means, and; (4) privacy and civil liberties considerations applicable to the particular dataset.

(U) NCTC Compliance also works collaboratively with NCTC CLPO and the Data Acquisition & User Group (DAUG), an NCTC-wide Governance Board responsible for the management and prioritization of data access, acquisition, and retention. The DAUG recommends new counterterrorism (CT) related datasets for acquisition, assesses the value of datasets already acquired by the Center, and provides recommendations on the Center's data acquisition, use, and retention to Senior Leadership.

(U) Each entity strives to ensure acquisition of and access to the counterterrorism- related datasets necessary for the Center's analysts to assess threats to the Homeland and U.S. interests abroad; determine the suitability of continued retention of the U.S. Person information; and the sufficiency and effectiveness of Safeguards applicability. Through the collaborative efforts of the above groups, NCTC and data-provider partners negotiated and signed the first Terms and Conditions (T&C) under the 2012 AGGs on 5 June 2013. Subsequently, NCTC and data-provider partners negotiated agreements for new or modified data ingestion and retention that were signed into effect on 25 November 2013, 27 November 2013, 19 June 2014, 2 October 2014, and 3 August 2015. NCTC performed a required periodic review of the appropriateness of continued retention and assessment of datasets replicated in accordance with Track 3 in August 2014, approximately one year after the first signed (T&C) subject to the 2012 AGGs see Attachment 1. This review, which was coordinated through the DAUG, and provided to the IC IG through DNI CLPO and DNI OGC, determined that continued data retention and assessment of the replicated datasets was appropriate. NCTC will next conduct such a review during fiscal year 2016 (FY16). We look forward to including the results of that review in our FY2016 Annual Report.

(U) As of the end of this reporting period, NCTC has not conducted bulk disseminations of U.S. Person information therefore, the required reviews to examine the continued necessity and efficacy of bulk disseminations is not applicable. Late in the reporting period, NCTC identified a compliance incident that initially appeared to involve the bulk dissemination of U.S. Person information to an IC partner for the purpose of assistance in determining whether the information contained Terrorism Information. Subsequent review of the matter determined that the subset of the dataset subject to the bulk disseminations did not, in fact, contain U.S. Person information. Should NCTC choose at some future point in time to consider engaging in bulk dissemination of U.S. Person information (as permitted under Sections IV (B) and (C) of the 2012 AGGs), NCTC will evaluate, on a case by case basis, the appropriateness of such requests, and fully review and report such activities in the proper annual report.

2. **(U) A general description of NCTC's compliance and audit processes[4]**

a. **Baseline Safeguards**

(U) The 2012 AGGs require that four specific Baseline Safeguards (BSGs) be applied to all datasets acquired pursuant to Track 3. Additionally, the AGGs require that all datasets replicated pursuant to Track 3 be considered for Enhanced Safeguards (ES), procedures, and audit mechanisms. Below is a brief discussion of each BSG and ES, and its associated audit and compliance review process. A discussion of the findings of those audits will be discussed in Section II.C. *Audit Findings and Identified*

[4] (U) 2012 AGGs, §VI.D.2(2)

*Shortcomings***.**

i. **(U) Baseline Safeguard 1:**

(U) *"These datasets will be maintained in a secure, restricted-access repository."*[5]

(U) For Baseline Safeguard 1 (BSG1), NCTC Compliance conducts semi-annual audits with a focus on privileged users who have system-administrator-like access to the secure, restricted access repositories where Track 3 datasets reside. We have chosen to focus on privileged users[6] because they are the only users that have accesses to data repositories and the ability to undertake changes and manipulations to the data. To ensure that privileged users understand the proper standards for usage and access to sensitive data, NCTC Compliance conducted extensive annual training for privileged users.

(U) To perform this audit, privileged user access is verified by evaluating five percent (5%) but no more than fifteen randomly selected logins from five percent of all Track 3 servers within a twenty-four hour period. The definition of privileged user's "LOGIN" has been redefined over time to be increasingly inclusive in the capture of logins for review. In FY14Q3 (April-June 2014), it was redefined to mean any activity performed by a privileged user on an audited server within a 15 minute interval. The new definition allowed for a more complete capture of login activity and information. Prior to this revision, NCTC Compliance found that privileged users move around servers with such frequency that tracking their activity created duplicative audit results. This process was again modified in FY15Q3 to further increase the number of logons reviewed by selecting, **at random, up to 15 unique users** from each of the 7 servers selected for audit. The 7 servers continue to be selected at random, via script, from all Track 3 servers with activity during the audit period. The selection of 15 unique users is a significant change to the BSG 1 audit processes as it removed the previous limit of 5% of the privileged logons (i.e. user activity performed within a 15 minute interval) and refocused to provide up to 15 unique privileged users who accessed each server on the given audit day.

ii. (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."*[7]

[5] (U) 2012 AGGs, §III.C.3.d(1)
[6] (U) Privileged Users refers to those personnel who have access to NCTC's IT systems that is beyond the level of access provided to the average end user (e.g. analysts, managers, support personnel). Examples of privileged users include systems administrators, database administrators, IT program/systems developers, and data scientists. Even among privileged users not all individuals hold the same level of privileged access.
[7] (U) 2012 AGGs, §III.C.3.d(2)

(U) NCTC's initial implementation of Baseline Safeguard 2 (BSG2) audit process centered on spot checks of various virtual groups. Each NCTC Directorate and Office managed membership in the virtual groups, as the groups were indicative of the missions of the groups, branches, and teams within the Directorates and Offices. With each group being unique based on mission and role, access to Track 3 datasets was approved and granted to individuals placed in these groups. Early BSG 2 implementation feasibility research suggested audits could be conducted to verify that the appropriate individuals were assigned to the correct groups. However, when conducting the audit, NCTC Compliance encountered significant challenges auditing the role-based access based upon the design of the groups and the membership process. These challenges will be further explained in Section II.C. *Audit Findings and Identified Shortcomings*.

(U) As a result of the lessons learned during the initial audit, NCTC transitioned to a by name access policy and process for dataset approval in Spring 2014. In FY15Q1 (November 2014), NCTC Compliance conducted a periodic audit and thoroughly reviewed every individual's assigned accesses. The audit found that 83% of the reviewed users possessed the appropriate roles to access Track 3 data. For users identified as having inappropriate roles, access roles were removed. There were 47 unverified individuals, who either transferred organizations or departed NCTC during the management review process. For those 47 individuals, we were unable to validate their roles for the audit period, therefore access was removed. Access removals were completed on 22 April 2015.

iii. (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."*[8]

(U) For Baseline Safeguard 3 (BSG3), NCTC defines "logons" as any query of or 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 verifies compliance with the BSG3 by sampling, on a semi-annual basis, all logons to all Track 3 datasets to ensure that the logons were authorized. If a logon is flagged as potentially unauthorized, the appropriate manager of the NCTC user from the Directorate or Office is notified to confirm that the activity in question was authorized. Logoffs are not independently tracked; the ending of a query or set of queries on a dataset will constitute a "logoff" from the dataset.

(U) Additionally as part of BSG3, NCTC also monitors, records, and audits all Track 3 dataset files/objects changes and manipulations to identify unauthorized

[8] (U) 2012 AGGs, §III.C.3.d(3)

file/object changes or manipulations. On a semi-annual basis, NCTC Compliance selects five (5) percent of all Track 3 servers with activity. An automated script runs to select five (5) percent, but not more than 15, changes/manipulations performed on the audited servers. To verify that each change/ manipulation is authorized, NCTC Compliance provides a record of each audited activity made to the appropriate supervisor for review. Supervisors review 100% of the changes and manipulations that can be attributed to a particular user in order to determine if the change/manipulation was authorized. The results are reported to NCTC Compliance. File/object changes and manipulations are only made by NCTC privileged users; no NCTC application provides end-users with the capability to make file changes or manipulations. Additionally, some file and object manipulations are machine-initiated as part of the extract, transform, and load (ETL) process needed to expose data to authorized users in NCTC applications. These changes and manipulations are also logged and may be captured for review as part of the audit process described above.

(U) Queries executed are monitored, recorded, and audited using NCTC's Baseline Safeguard 4 (BSG4) process described below.

(U) NCTC reviews, on a semi-annual basis, a sampling of the audit records captured for all accesses to, and manipulations of, Track 3 datasets to verify and document that no unauthorized accesses, modifications, or deletions are made to audit records. NCTC retains audit records 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.

iv. (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)"*[9]

(U) To ensure that queries against Track 3 datasets are narrowly tailored in accordance with the query design requirements of the 2012 AGGs, query reviews are conducted semi-annually by selecting queries run during a one month period within that audit period. Query reviews are conducted by Branch Chiefs from all branches with users who have activity against Track 3 data. Prior to conducting query reviews, Branch Chiefs must first attend

[9] (U) 2012 AGGs, §III.C.3.d(4)

mandatory Branch Chief Query Review Training, conducted by NCTC Compliance, to ensure both a clear understanding of the 2012 AGGs and examples of narrowly tailored queries.

(U) Once the designated audit month within the respective six month period has been chosen, NCTC Compliance executes an automated process by which all queries run against Track 3 datasets are extracted from NCTC Applications. As this could result in hundreds of queries, fifteen (15) are randomly selected for each branch. To facilitate and automate the query review process, NCTC Compliance created and manages a SharePoint site which serves as the Branch Chief Query Review interface where randomly selected queries are reviewed.

(U) During the Branch Chief review, each query is reviewed to ensure the design was solely to identify information reasonably believed to constitute terrorism information while minimizing the exposure of U.S. person data. As an additional protection, Branch Chiefs are not permitted to review their own queries. Should a Branch Chief's query come up as one of the 15 randomly selected queries for review in a given branch, a process is in place to have the review conducted by another Branch Chief/Manger. All non-compliant queries are reported to NCTC CLPO and Legal, and summarized results are forwarded to the NCTC Front Office.

b. (U) **Enhanced Safeguard (ES) Audits:**

(U) NCTC, in collaboration with DNI OGC, ODNI CLPO, and partner data providers has developed nine Enhanced Safeguards and associated audit processes to govern certain datasets that, due to their unique characteristics, require additional safeguards, procedures, and/or oversight mechanisms[10]. Below are descriptions of the nine (9_ Enhanced Safeguards and their audit processes developed to date.

i. (U) **Enhanced Safeguard-1:** ***Access to the datasets limited to a more restricted user group, based on roles determined in coordination with the data provider***
ES-1 is audited in quarters 1 and 3 of the fiscal year for those datasets subject to ES-1. This audit is conducted by obtaining a list individuals approved for access to datasets subject to ES-1 and cross comparing it against the list of all individuals who actually have access to that dataset(s). NCTC Compliance seeks to verify that all individuals with access to datasets protected by ES-1 were properly authorized and to identify any discrepancies between the two lists.

[10] Section III(C)(3)(e) of the 2012 AGGs states: *In addition to the requirements of paragraph (d), at the time when NCTC acquires a new dataset or a new portion of a dataset, the Director of NCTC or Designee shall determine, in writing, whether enhanced safeguards, procedures, and oversight mechanisms are needed. In making such a determination, the Director of NCTC or Designee shall (i) consult with the ODNI General Counsel and the ODNI Civil Liberties Protection Officer, and (ii) consider the sensitivity of the data; the purpose for which the data was originally collected by the data provider; the types of queries to be conducted; the means by which the information was acquired; any request or recommendation from the data provider for enhanced safeguards, procedures, or oversight mechanisms; the terms of any applicable international agreement regarding the data; the potential harm or embarrassment to a United States person that could result from improper use or disclosure of the information; practical and technical issues associated with implementing any enhanced safeguards, procedures, or oversight mechanisms; and all other relevant considerations.*

ii. (U) **Enhanced Safeguard -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)***

NCTC Compliance performs the ES-2 audit in quarters 2 and 4 of the fiscal year for those datasets subject to ES-2. The audit is conducted through submission of a formal inquiry to the NCTC ODSI Data Acquisition and Policy Group (DAP), NCTC Legal, and applicable NCTC directorates instructing them to report any non-TI disseminations that occurred during the reporting period, and whether any such disseminations were properly coordinated. If such disseminations occurred, NCTC Compliance confirms that coordination and approval occurred prior to dissemination. Additionally, NCTC Compliance reviews NCTC Current[11] and randomly selects fifteen finished intelligence (FININTEL) products to ensure non-Terrorism Information (TI) is not contained in the product.

iii. (U) **Enhanced Safeguard -3**: ***Access to the dataset contingent upon completing special training regarding use and handling of the specific data***

NCTC Compliance audits ES-3 in quarters 2 and 4 of the fiscal year for those datasets subject to ES-3. The audit consists of obtaining a list of all individuals approved for access to datasets subject to ES-3. Next, 15 names are selected at random to ensure those individuals completed the appropriate training prior to being granted access. Evidence of training completion is obtained from NCTC's compliance training and data access tracking database, BEACON[12], and the ODNI training management system.

iv. (U) **Enhanced Safeguard -4**: ***After _ years [13]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***

ES-4 is not currently applied to any dataset. In the event that ES-4 is applied to a dataset, NCTC Compliance will work with NCTC Mission Systems to develop the necessary audit processes.

v. (U) **Enhanced Safeguard -5**: ***After __ 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***

---

[11] (U) **NCTC CURRENT** is the classified website for the posting and dissemination of Counterterrorism (CT) reporting (cables) and analysis (finished intelligence) throughout the IC. As mission needs continue to evolve, NCTC's Office of Mission Systems continues to work closely with NCTC mission users to provide vital support. This tool has the feel of an online newspaper for CT professionals with a front page featuring titles, summaries, and graphics that highlight CT articles.

[12](U) Beacon is a database maintained by NCTC's Office of Data Strategy and Innovation Compliance and Transparency Group for the purpose of tracking NCTC personnel's completion of required compliance training and data access authorizations/removals.

[13] The timeframes referenced in ES-4, ES-5, ES-6, ES-7, ES-8, & ES-9 is determined separately for each dataset in consultation with DNI OGC, DNI CLPO, and the data provider at the time the ES is applied.

NCTC Compliance audits ES-5 in quarters 1 and 3 of the fiscal year for those datasets subject to ES-5. Only one dataset is currently subject to ES-5. In applying ES-5, to that dataset, NCTC opted for a more stringent approach than is strictly called for by ES-5. In this instance, the sensitive information within a dataset that necessitated ES-5 is not exposed to the general analytic population through any standard query tool. Instead, access to this sensitive data is granted on a case-by-case basis with supervisory approval and the proper mission need to know. The audit consists of querying the cognizant NCTC program office, NCTC MS application teams holding the data, and OSDI/DAP to determine if access requests for the sensitive data were submitted during the reporting period and, if so, whether proper access procedures were followed.

vi. (U) **Enhanced Safeguard -6**: ***More frequent reviews (every __ months) of the continued need to retain the dataset given the civil liberties and privacy concerns related to retention of the data***
ES-6 is not currently applied to any dataset. Upon enactment of this safeguard, NCTC Compliance will assess the ongoing need to retain the dataset and present the findings for review by the DAUG on an agreed upon frequency, in addition to the annual reviews. The assessment will be conducted using the same processes as for the annual reviews. Incorporation of all additional review requirements will be written into each individual dataset's Terms & Conditions.

vii. (U) **Enhanced Safeguard -7**: ***Additional spot checks (no less frequently than ___) to verify compliance with the enhanced access restrictions (See ES-1, above)***
ES-7 is automatically applied to any dataset to which ES-1 is applied. For the purposes of applying the additional spot check requirement of ES-7, NCTC will conduct an ES-7 audit every 6 months between the quarters in which ES-1 is audited. In practice, NCTC Compliance conducts ES-7 in quarters 2 and 4 of the fiscal year. As this is an additional check of ES-1, it is conducted using the same ES-1 processes.

viii. (U) **Enhanced Safeguard -8**: ***Additional spot checks (no less frequently than ___) to verify compliance with pre-dissemination coordination requirement (See ES-2, above)***
ES-8 is automatically applied to any dataset to which ES-2 is applied. For the purpose of applying the additional spot check requirement of ES-8, NCTC conducts an ES-8 audit every 6 months between the quarters in which ES-2 is audited. ES-8 is audited in quarters 2 and 4 of the fiscal year. As ES-8 is a spot check of ES-2, it is conducted using the same processes with one exception. Whereas in ES-2, NCTC Compliance queries NCTC Current and randomly selects fifteen FININTEL products to ensure non-Terrorism Information (TI) is not contained in the product, the ES-8 queries of NCTC Current are conducted against cables vice FININTEL products. This ensures that both FININTEL and cable products are each spot checked twice per fiscal year in quarters 1 & 3 (ES-2), and 2 & 4 (ES-8) respectively.

ix. (U) **Enhanced Safeguard 9**: ***Additional spot checks (no less frequently than ____) to ensure that no other searches of the dataset, other than those***

authorized pursuant to ES-4 (above), have been conducted during the previous period

ES-9 is not currently applied to any dataset. Since ES-9 is an additional spot check of ES-4, if/when ES-9 is implemented, it will be conducted using the same processes developed by NCTC Compliance and NCTC Mission Systems for ES-4.

3. (U) AUDIT FINDINGS AND IDENTIFIED SHORTCOMINGS

(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) Baseline Safeguard Audits Completed During Report Period

	FY13 Q4	FY14 Q1	FY14 Q2	FY14 Q3	FY14 Q4	FY15 Q1	FY15 Q2	FY15 Q3	FY15 Q4
BSG 1	X	X		X		X		X	
BSG 2	X	X		N[15]		X		X	
BSG 3	X		X		X		X		X
BSG 4	X	X		X		N[16]		X	

(U) BSG 1: During the reporting period (1 April 2013 – 30 September 2015), NCTC Compliance completed 5 BSG 1 audits, covering FY13Q4, FY14Q1 & Q3, FY15Q1 & Q3. For all audits, NCTC Compliance found that each privileged user login to Track 3 datasets was authorized.

(U) BSG 2: During the reporting period (1 April 2013 – 30 September 2015), NCTC Compliance completed 4 BSG 2 audits, covering FY13Q4, FY14Q1, FY15Q1 & Q3. BSG 2 auditing presented significant challenges and misleading data.

(U) BSG 2 was initially implemented through NCTC's role-based access policy wherein access to datasets was restricted by membership in pre-approved group member lists. The pre-approved group member lists originally served as group distribution lists (e.g. an email alias). NCTC Compliance adopted the lists for the dual use as Track 3 access control. This was done in lieu of creating another detailed list of personnel authorized for Track 3 data access. BSG 2 compliance verification was initiated in FY13Q4 (September 2013) with quarterly compliance verifications scheduled thereafter. As such, a quarterly BSG 2 compliance verification was again undertaken in December 2013/January 2014. During the first two compliance verifications, several challenges in the verification process were identified. Since the original purpose of the pre-approved member lists was to be an internal distribution list, many of the list "owners" responsible for list maintenance were unaware that they were being used for Track 3 data access. Several pre-approved, group-member lists had no "owner" or designated POC responsible for maintaining and updating the lists, as needed.

[14] (U) 2012 AGGs, §VI.D.2(3)
[15] (U) Audit not completed. Refer to discussion of Compliance Incidents Reporting.
[16] (U) Audit not completed. Refer to discussion of Compliance Incidents Reporting.

NCTC Compliance also found that many of the lists were not current and still held departed or reassigned individuals. This meant access lists were not maintained to the standard necessary to ensure appropriate individuals had access to Track 3 data and records were not kept documenting the addition and/or removal of individuals.

(U) As a result of the findings from the first two BSG 2 audits, as well as challenges identified in early audits of other BSGs related to the inability to accurately identify individuals' organizational affiliations in a timely manner, NCTC made two changes to its BSG auditing processes. First, in January 2014, NCTC modified the frequency of auditing from quarterly for all BSGs to staggered semiannual auditing wherein BSGs 1, 2, and 4 would be audited in fiscal year quarters 1 and 3 and BSG 3 would be audited in fiscal year quarters 2 and 4. Second, in Spring 2014, NCTC revised its data access policy to eliminate the utilization of pre-approved group member lists for granting access to Track 3 data.

(U) In support of the effort to move the Center to by-name access control, NCTC Compliance created roles for each Track 3 dataset and assigned users the data access roles on an individual basis. NCTC Compliance then discovered that it was not possible to obtain a valid listing of all individuals who support the Center (e.g. all categories of personnel (cadre, assignees, detailees, and contractors)) and their respective organizational assignment. Without such a listing, it was not possible to identify the appropriate managers to verify that individuals having Track 3 data accesses had the necessary mission need for such accesses. Due to the complexity of this issue, the challenge it presented could not be overcome in time to undertake the BSG 2 audit scheduled for FY14Q3 (June 2014). Although the BSG 2 verification in June 2014 was not completed, it was last completed in December 2013. NCTC Compliance reported and documented the missed BSG 2 audit as a compliance incident in accordance with the NCTC Compliance Incident Procedures.

(U) In FY15Q1 (November 2014), NCTC Compliance successfully extracted, from the Virtual Directory Engine (VDE), a list of all individuals with a Track 3 data role. With this information, NCTC Compliance created an audit report for each NCTC Directorate and Office for management review. Managers reviewed the report to determine if the listed individuals had a mission need for the identified Track 3 data access as of the date of the audit. Management review, completed on 8 April 2015, determined that 83% of the reviewed individuals appropriately possessed roles for access to Track 3 data. For users identified as holding inappropriate roles, such access was remediated by removal of all inappropriate accesses. Access removals concluded on 22 April 2015.

(U) Despite the missed FY14Q3 audit, NCTC's conduct of the BSG 2 audits remains consistent with the IC standard for auditing[17] based on the fact that NCTC undertook a BSG 2 audits in FY14Q1 and again in FY15Q1 with less than 1 year between the two audits.

(U) During FY15, NCTC Compliance initiated a series of actions to develop solutions to the challenges of auditing BSG 2 which will be discussed in further detail below. First, NCTC Compliance created a new database, Beacon, for the tracking of compliance training and data access authorizations and removals. This database replaced a more decentralized tracking process with a one-stop repository that improved the effectiveness of tracking, auditing, and

[17](U) Intelligence Community Standard Number 500-27 § E.2.c provides the requirement that agencies monitor the implementation of CIO standards at least annually.

reporting on compliance training and data access, as well as gaining efficiency in the process. Additionally, NCTC Compliance undertook a manual effort to review and update the organizational affiliation of all U.S. Government personnel reflected within NCTC IT systems, including the VDE. Additional changes, including the review and updating of all contractor affiliations, will continue in FY16 and are further discussed in Section I, *A description of any material changes or improvements NCTC implemented, or is considering implementing, to improve compliance with these Guidelines*, below. .

(U) For the FY15Q3 BSG 2 Audit, NCTC Compliance focused on auditing the training requirement mandated by the AGGs[18]. NCTC Compliance again extracted a list of individuals with each Track 3 data role from the VDE and compared it to each individual's training record in the VDE and Beacon. The audit sought to verify that all assigned individuals completed NCTC U.S. Persons training as required by the 2012 AGGs in BSG 2[19], three (3) NCTC mandatory compliance training courses (Data Access and Use, Privacy Act, and Foreign Intelligence Surveillance Act), and any appropriate dataset-specific training[20] required in the data provider agreements (i.e. Terms & Conditions). The audit report highlighted all individuals determined to be missing compliance training or dataset-specific training. Of the reviewed individuals, 87% of the reviewed users possessed required the training required for their identified Track 3 data access. Three (3) users were identified as being non-compliant with the required training policies. Two immediately completed necessary training and the third had a planned August 2015 departure from the Center. Approximately 12% of the individuals were identified as having departed NCTC, changed responsibilities, or their NCTC organizational affiliation could not be determined. For these individuals, their data accesses were immediately removed. No additional remediation was determined to be necessary. This was the first time NCTC Compliance audited the training requirement as part of BSG 2 auditing processes. The ability to undertake and successfully complete this audit was the direct result of process improvements NCTC Compliance executed to improve the implementation of BSG 2.

(U) **BSG 3:** During the reporting period (1 April 2013 – 30 September 2015), NCTC Compliance completed 5 BSG 3 audits, covering FY13Q4, FY14Q2, FY14Q4, FY15Q2, and FY15Q4.

(U) As noted in the discussion of BSG 3 in Section II(B), *A general description of NCTC's compliance and audit processes,* above, NCTC defines "logons" as any query of or 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 verifies compliance with BSG3 by sampling, on a semi-annual basis, all logons to all Track 3 datasets to ensure that the logons were authorized. If a logon is flagged as potentially unauthorized, the appropriate manager of the NCTC user from the Directorate or Office is notified to confirm that the activity in question was authorized. Logoffs are not independently tracked; the ending of a query or set of queries on a dataset will constitute a "logoff" from the dataset.

[18] (U) 2012 AGGs, §III.B(3) and §III C(3)(d)(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 11I.B.3**." (emphasis added).
[19] (U) 2012 AGGs, §III.B(3) and §III C(3)(d)(2)
[20] (U) 2012 AGGs, §III.B(2)(a), (b), and (c) and §III(B)(2)

(U) During the FY13Q4 audit all supervisors reviewing potentially unauthorized accesses found that all were in fact authorized. NCTC Compliance notes that one (1) of those accesses was conducted by a former NCTC analyst on detail to the Center from a partner agency who returned to the Center shortly after returning to his/her home agency and accessed NCTC IT systems to conduct the query in an effort to assist NCTC in closing out a project initiated during the analyst's tenure at NCTC. NCTC Compliance remediated this effort by working to ensure data and computer system accesses are removed more quickly upon an individual's separation from the Center, regardless of reason.

(U) The FY14Q2 audit identified one (1) unauthorized search. That search was the result of a saved search running within an analytic query tool against a previously authorized dataset. The user had since changed responsibilities and no longer had a mission need for access to that data. The application running the saved query was determined to be checking users' data access credentials before returning query results, thus no invalid/unauthorized search results were presented to the user. In investigating this issue, NCTC Compliance discovered the application in question checked user data access credentials after query submission for all queries, not just saved queries. In all searches, the application then filtered the returned results based on an analyst's approved dataset roles in the VDE. As a result of the authentication process implemented by this application, queries flagged falsely as invalid because of the authentication process. In consultation with NCTC Legal and NCTC CLPO, NCTC Compliance worked with Mission Systems to redesign the application to implement user authentication upfront prior to query submission in order to better protect Track 3 data. This change significantly reduced the number of invalid accesses presented for validation beginning with the FY14Q4 audit. With regard to the identified invalid access resulting from the saved search, that matter was remediated by removal of the saved search from the application.

(U) It should be noted that the false-positive, invalid accesses that were reviewed in FY14Q2 served a valuable purpose for NCTC Compliance as they identified a gap in analyst understanding regarding the datasets available; the data access process, particularly for datasets where both Track 1 and Track 3 access are available; and individuals' understanding of the delta between their accesses and the accesses available to them. NCTC Compliance continues to work to improve awareness of the datasets available within the Center and to streamline the process for requesting and granting accesses.

(U) A second issue regarding false positives was identified during the FY14Q2 audit. These false positives were the result of NCTC and non-NCTC federal partner agency personnel gaining access to Track 3 datasets by virtue of their membership in an inter-agency screening program. As a result of the way in which data access was granted in this particular program, NCTC Compliance was unable to verify the whether the users were properly authorized for the Track 3 data access. With limited exception, access to Track 3 data is authorized and granted via an NCTC Compliance process implementing NCTC's Role-based Access Policy. Access to the application used in the screening program and the dataset in question within the tool was previously an exception to this process in that the program team previously granted access to both the application and the data. NCTC Compliance, in consultation with NCTC Legal and NCTC CLPO, worked with Mission Systems and the program office to bring this program in-line with the data access authentication processes used by other NCTC applications wherein the dataset was assigned a data access role and individuals were added to

it individually through the standard process managed by NCTC Compliance. The modified access authentication and access granting processes for NCTC personnel were implemented in February 2015 thereby reducing the number of false positives for NCTC personnel. The modifications impacting non-NCTC personnel's access to Track 3 data through this screening program are ongoing.

(U) In addition, while these data accesses by non-NCTC personnel were likely envisioned when the screening program was initiated, they were not accounted for in the T&Cs under which the data is secured, and given that these personnel are not operating under NCTC's authorities, these accesses are technically considered disseminations, in violation of the underlying T&Cs. In October 2014, the data provider acknowledged USG partner access to the screening program and concurred with NCTC's determination that such access is considered a dissemination thereby excluding the USG partners from NCTC's baseline safeguard, enhanced safeguards, and training requirements. The data provider further advised that they consider such sharing to be subject to separate MOUs between the data provider and the USG partners stipulating data confidentiality, access, handling and dissemination provisions and requirements. Thus, while the non-NCTC personnel flag as having invalid access on the audit reports based on the way in which the data is pulled, NCTC Compliance has not attempted to verify these accesses. In the future, NCTC Compliance may develop a process by which the list of non-NCTC users is provided to a point of contact at each agency for validation. NCTC is also working with the data providers to draft addenda to the T&Cs addressing this issue.

(U) FY14Q4 audit found that all potentially unauthorized logons/accesses were in fact authorized as the individuals should have had access to the datasets being queried. NCTC Compliance remediated all of the potentially invalid accesses reviewed by processing the identified individuals for the dataset access in question. As noted above, the number queries flagged as potentially invalid accesses that were determined to be false positives was significantly reduced this quarter.

(U) In the FY15Q2 audit, five of the six managers who reviewed potentially invalid accesses determined that the accesses were authorized. Four of those five managers further indicated that the individuals should have had access to the datasets being queried. The sixth manager, indicated the accesses in question were unauthorized, but the manager further noted that the individuals should have had access to the datasets in question. NCTC Compliance remediated all of the potentially invalid accesses reviewed by processing the identified individuals for the dataset access in question.

(U) In the FY15Q4 audit, the managers reviewing the potentially invalid accesses determined that four analysts had requested data scientist deep-diver queries of Track 3 datasets for which the requesting analyst lacked authorization. Three of those analysts were determined to have Track 1 (native) access to those datasets. Thus, the access was deemed to be authorized and the analysts were processed for Track 3 data access in addition to the previously authorized Track 1 access. The fourth analyst was determined to have not actually accessed or received data from the dataset in question, but had inquired as to the delivery and deletion of data from that dataset by the data science team in order to document a compliance incident in accordance with the NCTC Compliance Incident procedures. Thus, no remediation was necessary with regard to the 4th individual.

(U) NCTC Compliance found auditing BSG 3.2, file and object changes and manipulations, to be extremely challenging. Machine-to-machine interactions and human-to-machine interactions are indistinguishable in the audit logs using the Center's current logging and audit software. This means that the routine machine processing of data to make it available to analysts looks the same as nefarious human-initiated changes to the data in the audit logs. Thus, it is extremely difficult to determine whether a privileged user accessed a server, and even harder to know whether that user was authorized to do so, and whether any data was changed during their access. Additionally, privileged users have the ability to alter server logs meaning that if they are involved in nefarious activity they also have the ability to alter the logs to hide their activity further increasing the difficulty in identifying unauthorized changes and manipulations of the data.

(U) During the FY13Q4, FY14Q2, and FY14Q4 audits, all changes and manipulations submitted for management review were deemed to be authorized.

(U) Between the FY14Q4 and FY15Q2 audits, a number of changes occurred within NCTC Mission Systems management. While some of the managers continued to review and deem authorized the changes and manipulations events forwarded to them for review, several of the new managers raised concerns about their ability to make compliance determinations in support of the BSG 3.2 audits. As a result, during the FY15Q2 audit, 58.5% of the changes and manipulations submitted for review, were not fully reviewed and no compliance determinations (i.e. authorized or not authorized) were made for these changes and manipulations. The remaining 41.5% of the changes and manipulations reviewed were deemed authorized. Similarly in FY15Q4, 49.2% of the changes and manipulations submitted for review were deemed to have been authorized. The remaining 50.8% of the changes and manipulations submitted for review, were not fully reviewed and no compliance determinations (i.e. authorized or not authorized) were made for these changes and manipulations due to the non-attributable nature of the events.

(U) NCTC Compliance will be working during FY16 to design, test, and implement improved means of logging and reviewing file and object manipulations in order to more effectively undertake these audits.

(U) Unlike BSG 3.1, and 3.2, BSG 3.3, audit of the audit, was only conducted 4 times during the reporting period. BSG 3.3 audits did not began until FY14Q2. The audits completed for FY14Q2, FY14Q4, FY15Q2, and FY15Q4 found no unauthorized accesses, modifications, or deletions to the audit records.

(U) **BSG4:** NCTC Compliance conducted the first BSG 4 audit in FY13Q4 and randomly selected 465 queries for review. Twenty-seven (27) queries were not reviewed because of the analyst's organizational affiliation could not be determined in a timely manner and several reviewers did not know the analyst who performed the query (usually as the result of a recent move by the supervisor or analyst into/out of an organization). Of the 438 queries actually reviewed, only 11 queries were deemed non-compliant. Five (5) of the 11 queries were not narrowly tailored and the remaining six (6) involved analyst error. In addition, nine (9) of the 438 queries were performed by the trainer for compliance training purposes and 45 of the 438 queries were submitted for testing and/or technical support.

(U) During FY14 Q1, BSG 4 was again audited with 515 queries randomly selected for review. Initially, reviewers deemed all 515 queries compliant. Upon closer examination with one branch chief, NCTC Compliance found seven (7) queries non-compliant. NCTC Compliance found that six (6) of those queries were not narrowly tailored and one (1) resulted from analyst error.

(U) During FY15 Q1, NCTC Compliance did not conduct a semi-annual BSG 4 audit. Due to the excessive time required to accurately identify the organizational assignments of the analysts whose queries were selected for review, the data was too stale to obtain accurate management reviews of query compliance. As a result, NCTC Compliance submitted a compliance incident for failure to audit as required.

(U) For the FY15Q3 audit, NCTC Compliance randomly selected 790 queries for manager review. Managers determined approximately 88% of the queries were compliant, and 9% were non-compliant. Analysts with queries identified as non-compliant during this review, were counseled, corrected and retrained. Twenty-seven (3%) of the queries could not be verified because the analysts who performed the queries moved organizations during the management review process.

(U) An additional review conducted by NCTC Compliance found that some queries determined by managers to be compliant, were in fact, non-compliant. The primary issue identified by NCTC Compliance, leading it to overturn the managers' initial determinations that queries were compliant, was that the analyst had queried the incorrect dataset(s) for the data being sought. In order to mitigate future such occurrences, NCTC Compliance will distribute reminder guidance for proper queries and begin publishing a newsletter highlighting common query problems and tips along with additional guidance to benefit analysts and managers as they make use of data. In the past, all remediation had been conducted at the individual analyst/branch chief level. The creation of this newsletter will allow for broader sharing of lessons learned in the future.

(U) It should be noted that an application, by design, prevented individuals from limiting the Track 3 datasets searched during a fielded search for document ID number (DOCID). Instead, the application searched against all datasets available to the user. For this reason, managers have marked DOCID searches as compliant. Since this review, in July of 2015, NCTC deployed an update to the application that provides users the ability to select only the datasets they want to search and thus allowing appropriately limited and narrowly tailored searches.

(U) The design of a second analytic tool similarly prevents analysts from narrowly tailoring their searches. This particular tool is designed to better analyze entities and it does this by aggregating known data around the entity of interest. The tool refers to each entity being analyzed as a "case". Datasets that analysts want to query in support of their analysis must be added to the "case" as a potential data source. Once a particular dataset is added as a potential source to the analytic "case" for a particular entity, all searches conducted within that "case" query against all datasets associated with the "case". Analysts are presently unable to de-select datasets without completely removing the dataset(s) from the "case". NCTC continues to explore IT development solutions that would allow for analysts to more narrowly tailor their queries when using this important analytic tool.

(U) **Dataset Enhanced Safeguard (ES) Audit Findings:**

(U) Enhanced Safeguards Audited by Audit Period

	Sept. 2014	Dec. 2014	March 2015	June 2015	Sept. 2015
ES 1		**X**			
ES 2	**X**		**X**		**X**
ES 3	**X**		**X**		**X**
ES 4	**Not Applied**				
ES 5		**X**		**X**	
ES 6	**Not Applied**				
ES 7	**X**		**X**		**X**
ES 8		**X**		**X**	
ES 9	**Not Applied**				

(U) ES-1: As described above, ES 1 ensures compliance by limiting datasets to a more restrictive user group, as agreed upon between NCTC and the data provider. This audit has been applied to one dataset. ES 1 was first audited in December 2014, and was audited twice during the reporting period (FY15Q1 (December 2014) and FY15Q3 (June 2015)). During both audit quarters, NCTC Compliance found that the dataset subject to ES 1 was non-compliant. ES 1 is intended to verify that access to a particular dataset is subject to a more restricted user group. With limited exception, access to Track 3 data is authorized and granted via ODSI Compliance and Transparency Group's (CTG's) processes, implementing NCTC Policy 4: Role-Based Access, wherein completion of all NCTC mandatory compliance training and all dataset-specific training is verified prior to authorizing/granting access to that specific dataset. Access to the sole dataset subject to ES 1 was instead granted by the NCTC mission directorate responsible for the IT tool used to access the data based on mission need, but outside of the standard ODSI data access process. At the time of the December 2014 audit, the mission team did not require or verify completion of the NCTC mandatory training or the dataset-specific training prior to granting access to the dataset. The mission team also did not keep appropriate records documenting the approval of individuals granted access to the dataset in order to facilitate NCTC Compliance's ES 1 audits.

(U) In February 2015, NCTC Mission Systems deployed an update to the referenced IT application used to analyze the dataset subject to ES 1 thereby bringing the dataset and application in line with NCTC Policy 4 and the ODSI-managed data access process. This in turn, facilitated the necessary ES 1 auditing. The June 2015 audit reviewed 174 instances of access to the dataset in question. The application used to access the referenced dataset is available on two different IT networks, so some individuals have access on both networks. The June audit found that 21 individuals had the necessary data access role for the particular Track 3 dataset without documentation as to being authorized for that data role. Additionally, NCTC Compliance identified 46 instances, involving 34 individuals, where a compliance determination could not be made because the NCTC/ODSI database used to track access authorizations indicated access was authorized, but lacked information regarding the authorization date[21]. NCTC Compliance also identified 11 former staff and contract personnel

[redacted]

who had departed the Center but still showed as having valid data access roles. This was remediated through removal of those 11 individuals' data access roles.

(U) It is should be noted that the non-compliance is mitigated by the fact that the data fields that were the basis for ES 1 have never been exposed in the analytic tool and no analyst has ever made a request for access to that data.

(U) Additionally, certain NCTC federal partner agencies also have access to this dataset via the NCTC IT application. Non-NCTC users are nominated for access by their respective agencies based on mission need. NCTC Compliance, in coordination with NCTC CLPO, NCTC Legal, and the NCTC mission directorate will be developing a process for periodic revalidation of those individuals' continued mission need. It is anticipated that these periodic revalidations will be undertaken at the same time as the semi-annual ES 1 audits.

(U) **ES-2**: As described above, ES 2 requires advance coordination with the data provider and NCTC Legal prior to any dissemination of non-terrorism information derived from subject datasets. Six (6) datasets are subject to ES 2. For this reporting period, audits were conducted in FY14Q4 (September 2014), FY15Q2 (March 2015), and FY15Q4 (September 2014). During all three audits, NCTC Compliance identified no occurrences of non-TI disseminations in finished intelligence products based on responses from the NCTC directorates and offices, NCTC Legal, and NCTC ODSI/Data Acquisition and Policy (ODSI/DAP), and spot checks of FININTEL products posted to NCTC CURRENT.

(U) During the FY14Q4 audit, NCTC Compliance considered whether the transmittal of the fact that certain applicants for U.S. Government immigration benefits as identified in datasets subject to ES 2 have, in fact, "not been flagged for review" by NCTC's screening and vetting process. And whether that constitutes a dissemination of non-TI information even though the transmittal of that data is contemplated by and consistent with the screening and vetting process. When consulted, the data provider advised that the agency is aware of and agrees to such data transmittals. In reviewing the data provider's response with NCTC Legal and NCTC CLPO, NCTC Compliance determined that such transmittals are non-TI disseminations lacking documentation in appropriate data provider agreements. As such, NCTC Compliance determined that the screening and vetting process was not in compliance with ES 2 with regard to two datasets. Having identified this gap in the data provider agreements, NCTC/ODSI/DAP will be working with the NCTC mission directorate and data provider to update these documents. In the interim, NCTC continued to transmit these disseminations based on the intent of the data providers.

(U) Additionally, as discussed in Section A "Periodic Reviews", NCTC Compliance learned late in the reporting period that, since 2010, NCTC has been making bulk disseminations of a non-U.S. Person subset of an immigration-related dataset subject to ES 2, to another federal

[redacted]

agency for the limited purpose of having that agency assist NCTC in determining whether the subset of the dataset contains TI. Those disseminations are not explicitly authorized in the data provider agreement and have not been authorized on a case-by-case basis with the data provider and NCTC Legal. As a result, those disseminations are non-compliant with ES 2. As noted in Section A above, NCTC continues to work with the data provider to update the data provider agreement authorizing these disseminations.

(U) **ES-3**: As described above, ES-3 requires that access to subject datasets be contingent upon completion of special training regarding use and proper handling of the specific dataset. NCTC Compliance performed audits in FY14Q4, FY15Q2, and FY15Q4. Three (3) datasets are subject of ES 3.

(U) With limited exception, access to Track 3 data is authorized and granted via NCTC Compliance processes implementing NCTC's Role-Based Access policy, wherein completion of all dataset-specific training is verified prior to authorizing/granting access to that specific dataset. ES 3 auditing encountered the same challenge as did ES 1 auditing with regard to a particular Track 3 data set that was processed outside of the standard process. Access to a particular analytic application and the particular Track 3 dataset (subject to ES 3) within the application was an exception to this process in that the NCTC directorate tool owner granted access to both the tool and the data within the tool. For the FY14Q4 ES-3 audit, the owners of the tool did not require nor verify completion of required dataset training prior to granting access to the database. For this reason, the program was determined to not be in compliance with ES 3.

(U) Prior to the FY15Q2 ES 3 audit, NCTC Compliance worked with the data program in question, to transition program access control processes for the data within the tool to the standardized processes and data access roles used throughout the Center[22]. In early February 2015, the program moved the NCTC users of this data to the standardized access control process and data roles. As such, NCTC Compliance was able to verify that the dataset was in compliance with ES 3in FY15Q2. NCTC Compliance continues to work with the data program to implement standardized access control processes on the portion of the tool used by NCTC's U.S. Government partners in this program.

(U) The other two datasets subject to ES 3 were determined to be compliant in all 3 audit periods.

(U) **ES-4:** Not applied during the reporting period.

(U) **ES-5:** As described above, ES 5 audits confirm that after a specified period of time, NCTC has employed privacy enhancing technologies/techniques which allow USP information or other sensitive information to be "discovered" without providing the content of the information, until the appropriate standard, is met. Only one (1) data was subject to ES 5 during the reporting period. NCTC Compliance conducted one catch-up audit covering FY15Q1 (December 2014) and FY15Q3 (June 2015) on the subject dataset. NCTC Compliance determined that no sensitive data was exposed in any analytic tool and no analyst

[22] Standardized and dataset specific user roles are established and utilized throughout the Center. Each dataset is assigned a unique user role (e.g., name) and that user role is the only user role that will allow access to the specified dataset, regardless of the tool utilized to make the data available.

requested access to the data during the audit period. Thus, NCTC's handling of the subject dataset is compliant with ES 5.

(U) **ES-6:** Not applied during the reporting period.

(U) **ES-7:** As described above, ES 7 is an additional spot check no less frequently than every 6 months to verify compliance with the enhanced access restrictions of ES 1. During the reporting period, NCTC had one (1) dataset subject to ES 7 (and ES 1). During the reporting period, NCTC Compliance, conducted three (3) audits of ES 7 for FY14Q4 (September 2014), FY15Q2 (March 2015) and FY15Q5 (September 2015). ES 7 auditing faced the same challenges already discussed for ES 1 and ES 3. Specifically, at the time of the FY14Q4 ES 7 audit, access to the sole dataset subject to ES 7 was granted by the NCTC mission directorate responsible for the IT tool used to access the data based on mission need, but outside of the standard ODSI data access process. As a result, the FY14Q4 ES 7 audit found that the dataset was not in compliance with ES 7 because access was granted outside the standard NCTC/ODSI access process, without necessary verification of mandatory compliance and dataset-specific training, and without appropriate documentation of accesses granted and removed.

(U) NCTC Compliance worked with the program in question to transition their access control processes for the data within the tool to the standardized processes and roles used throughout the Center. As described in the ES 1 section above, in February 2015, NCTC Mission Systems deployed an update to the referenced IT application used to analyze the dataset subject to ES 1 thereby bring the dataset and application in line with NCTC Policy 4 and the ODSI-managed data access process. This in turn, facilitated the necessary ES 7 auditing. The FY15Q2 (March 2015) audit reviewed 212 instances of access to the dataset in question. The application used to access the referenced dataset is available on two different IT networks, so some individuals have access on both networks. The March 2015 audit found 38 instances, involving 31 individuals, of non-compliance where individuals were granted access to the data without being authorized for that data access through the NCTC/ODSI data access process. NCTC Compliance identified another 47 instances, involving 35 individuals, where a compliance determination could not be made because the NCTC/ODSI database used to track access authorizations indicated access was authorized, but lacked information regarding the authorization date[23]. NCTC Compliance also identified 14 former staff and contract personnel who have departed the Center but still had valid data access roles for the dataset. This was remediated through removal of those 14 individuals' data access roles in August 2015.

[redacted]

(U) It is should be noted that the above described non-compliance is mitigated by the fact that although access is defined as the data "could" have been accessed, the data fields that were the basis for ES 7 have never been exposed in the analytic tool and no analyst has ever made a request for access to that data.

(U) The FY15Q4 (September 2015) audit identified no instances of non-compliance wherein NCTC personnel had access to the data outside of the ODSI-managed data access process. NCTC Compliance did identify 21 former staff and contract personnel who have departed the Center but still had valid data access roles for the dataset. These accesses were remediated in November 2015 when updated access control processes were implemented for the dataset subject to ES 7.

(U) Additionally, as noted in the ES 1 section above, certain NCTC federal partner agencies also have access to this dataset via the NCTC IT application. Non-NCTC users are nominated for access by their respective agencies based on mission need. NCTC Compliance, in coordination with NCTC CLPO, NCTC Legal, and the NCTC mission directorate will be developing a process for periodic revalidation of those individuals' continued mission need. It is anticipated that these periodic revalidations will be undertaken at the same time as the semi-annual ES 7 audits.

(U) **ES-8**: ES 8 is an additional spot check (no less frequently than every 6 months) to verify compliance with the pre-dissemination coordination requirement of ES 2. Six (6) datasets were subject to ES 8 during this reporting period. ES 8 was audited for FY15Q1 (December 2014), FY15Q3 and (June 2015). NCTC Compliance identified no occurrences of non-TI disseminations in NCTC cable products based on responses from the NCTC directorates and offices, NCTC Legal, and NCTC/ODSI/ DAP, and spot checks of cables posted on NCTC CURRENT.

(U) As discussed above in the ES 2 section, during the FY14Q4 ES 2 audit (which is spot checked by ES 8), NCTC Compliance considered whether the transmittal of the fact that certain applicants for U.S. Government immigration benefits identified in datasets subject to ES 2 have "not been flagged for review" by NCTC's screening and vetting process. And whether that constitutes a dissemination of non-TI information even though the transmittal of that data is contemplated by and consistent with the screening and vetting process. When consulted, the data provider advised that the agency is aware of and agrees to such data transmittals. In reviewing the data provider's response with NCTC Legal and NCTC CLPO, NCTC Compliance determined that such transmittals are non-TI disseminations lacking documentation in appropriate data provider agreements. As such, NCTC Compliance determined that the screening and vetting process was not in compliance with ES 8 with regard to two datasets for both the FY15Q1 and FY15Q3 audit periods. Having identified this gap in the data provider, NCTC/ODSI/DAP is working with the NCTC mission directorate and data provider.

(U) Additionally, as discussed in Section A "Periodic Reviews" and the ES 2 section above, NCTC Compliance learned late in the reporting period that, since 2010, NCTC has been making bulk disseminations of a non-U.S. Person subset of an immigration-related dataset, subject to ES 2, to another federal agency for the limited purpose of having that agency assist NCTC in determining whether the subset of the dataset contains TI. Those disseminations are not explicitly authorized in the data provider agreement and have not been authorized on a

case-by-case basis with the data provider and NCTC Legal. As a result, those disseminations are non-compliant with ES 8. As noted in Section A above, NCTC continues to work with the data provider to update the appropriate data provider agreement authorizing these disseminations.

(U) **ES-9:** Not applied during the reporting period.

(U) Compliance Incident Reporting

(U) NCTC has a robust process for the reporting, review, and remediation of compliance incidents. In accordance with that process, all data handling compliance incidents are reported to the data provider, NCTC Legal, and NCTC CLPO. When the appropriate thresholds are met, incidents are also reported to the President's Intelligence Oversight Board (IOB), and the IC Inspector General and Department of Justice[24].

(U//~~FOUO~~) In addition to documenting facts of each incident, the reports also characterize each incident using standard categories in order to better identify trends across incidents and improve remediation efforts. As noted on the chart below, during this reporting period, fifty-three (53) compliance incidents were discovered.

(U) Compliance Incidents by Type and Cause of Incident

CAUSE OF INCIDENT	Type of Compliance Incident					
	Late Deletion	Late Delete & Unauthorized Data Receipt	Inappropriate Access[25]	Inappropriate Dissemination	Inappropriate Search	Failure to Audit
Communication, Human Error, Process	3		1			
Communication, Data Provider Error, Misinterpretation/ Misapplication of Statute,		1				
Communication & Process	2	1				
Human Error	4			1		
Human Error & Process	15		1			
Human Error & Scrip/Coding Error	1					
Human Error & Training					3	
Human Error, Training & Process	1			1		

[24] (U) 2012 AGGs, §VI.D.1.

[25] (U) Inappropriate access includes individuals being inappropriately authorized for data access, individuals retaining access when access is no longer appropriate, and the failure to apply/implement appropriate access controls.

Process	5		1			2
Process & Technical	4					
Script & Coding Error	3					
[redacted]nical Failure	1					
Technical Failure, Training, & Process	1					
Training & Process			1			
TOTAL	40	2	4	2	3	2

(U) **Late Deletion:** Of the 53 incidents reported during this reporting period, 40 incidents (75%) were late deletions. Late deletions refer to data that was retained on NCTC IT systems beyond the temporary time authorized by the AGGs or the data provider agreement, whichever is shorter. In none of these instances was the cause of the late deletion an intentional disregard for the authorized retention period. Instead, late deletions most frequently result from a combination of human and process error wherein ongoing IT development and systems administration work to continually update and improve NCTC IT systems, improve use of existing data through the use of new analytic tools, or to bring in new datasets or data fields within an existing dataset, make some change to the existing IT scripts or physical location of the data on the IT systems that breaks the deletion processes. Such instances generally result from a privileged user's (IT developer or systems administrator) failure to follow standard operating procedures (SOPs) regarding the documentation of the relocation/movement of data or the testing of pre-existing code to ensure it was not negatively impacted by new code. In remediating such incidents, NCTC Compliance works with Mission Systems to identify modifications that can be made to existing SOPs to minimize the likelihood of repeating the same issue. The implementation of the Data Catalogue which documents data storage locations and retention periods for each data set, along with implementation of 7-day advance deletion, and post-deletion spot checks to ensure data was in fact deleted on the planned date have reduced the frequency of late deletion events during the course of this reporting period.

(U//~~FOUO~~) Failure to Audit: NCTC experienced several challenges while conducting audits and spot checks of the Baseline Safeguards during this reporting period. As discussed above and in our previous report, BSG 2 is implemented through NCTC's role-based access policy based on membership in pre-approved virtual groups (generally, broken out by offices within an individual NCTC Directorate) and 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 the course of auditing BSG 2, beginning in FY13Q4, NCTC discovered that the lists were not being properly maintained to the standard required for access control purposes. In many cases, the lists were originally intended to serve as group distribution lists (i.e. email aliases) for internal communication purposes and the list "owners" were unaware the lists had also been adopted for access control purposes. As a result, individuals departing a group were not being removed in a timely manner. [redacted] As a result, the lists provided only a snapshot in time on the date an audit was conducted. As a result of the challenges in auditing BSG 2 and other BSGs, in early calendar year 2014, NCTC Compliance decided that NCTC would no longer audit every BSG every

quarter. Instead, effective FY14Q2, BSG auditing would be staggered so that each BSG was audited twice a year. More specifically, BSG 2 would be audited in quarters 1 and 3 of the fiscal year.

(U) In addition, given the ongoing challenges encountered with role based access, NCTC Compliance determined it was necessary that NCTC transition to by-name access control. In the spring of 2014, NCTC revised its data access policy to account for this change and the pre-approved group member lists were no longer used to grant access to Track 3 data.

(U) NCTC Compliance recognized, however, that before the BSG 2 compliance verification process could be revised to transition to a by-name verification process, that a valid listing would be needed of all individuals who supported the Center, to include all categories of personnel (cadre, assignees, detailees, and contractors) and their respective assignment, down to the L5 or branch level, and that a mechanism was needed, before verification could begin, to ensure that such a listing was properly maintained and regularly updated. Because an authoritative roster of government and contractor personnel could not be generated for comparison against the data access list, the FY14Q3 audit and the audit was not conducted. NCTC Compliance documented this incident and reported it in accordance with NCTC Compliance Incident Procedures.

(U) NCTC Compliance has since developed a set of manual and automated processes combined with regular updates as a full step towards identifying the assigned organization of personnel in the Center. Even with these small process improvements, NCTC Compliance has already reduced a large number of individuals whose organizational affiliations must be researched during auditing. BSG 2 has since been audited in FY15Q1 and FY15Q3. Additional improvements are planned for FY16 and are further discussion below in Section II.I. *A description of any material changes or improvements NCTC implemented, or is considering implementing, to improve compliance with these Guidelines.*

(U) Similarly, in FY15Q1, NCTC Compliance failed to audit BSG 4 due to the same challenge identifying personnel organization affiliations. Due to the excessive time introduced into the auditing process researching organizational assignments in order to properly route selected analyst queries for review, the queries were too stale to be properly reviewed. Thus NCTC Compliance did not complete the audit. NCTC Compliance documented this incident and reported it in accordance with NCTC Compliance Incident Procedures.

4. (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;***[26]

(U) NCTC continues to utilize the same data deletion tools for automated removal of data subject to both the 2008 and 2012 AGGs.

[26] (U) Id., §VI.D.2(4)

(U) To ensure compliance with the requisite deletion rules, the NCTC Data Management Team (DMT)[27] uses the Data Catalog[28] to track and monitor planned and actual data deletion dates. To ensure Center compliance, the DMT sends a weekly broadcast email to all entities within the Center who have access to data with near-term deletion dates. Email notifications for the given item begin four weeks prior to the scheduled deletion date, and occurs on a weekly basis thereafter, to ensure that the entities are aware and mindful of the imminent and upcoming deletion due date and can plan accordingly.

(U) All Center entities that 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 when their data is due for deletion. Within MS, Data Services[29] (formerly the Data Factory) is responsible for logging all data deletions into a central database. Both DMT and Data Services will use this database, in addition to audits and spot checks, to verify that required deletions occurred as planned.

(U~~//FOUO~~) During this reporting period, the Center approved the deletion of Track 3 data seven days prior to the required deletion date in attempts to ensure that all data is timely deleted and that delayed deletions can be discovered and remedied within the allowed retention period. Two exceptions have been made. One exception has been made for a specified dataset wherein the data is deleted fourteen days prior to the required delete date given the size of the dataset and time needed to delete. The second exception has been made for NCTC's new correlation system where data is deleted three (3) days prior to the required delete date. The new correlation system includes a robust lifecycle management process that includes daily reporting on data ingested and deleted within the previously 24 hours. Based on the availability of daily reporting regarding the status of data deletions, the decision was made that three (3) days advance deletion is sufficient.

5. (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 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***

[27] (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 manual delivery of each dataset and posts both the receipt date and planned and actual deletion dates in the Data Catalog.
[28] (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.

[redacted]

under section IV.B.2;[30]

(U) As of the end of the reporting period, NCTC has not disseminated U.S. Person information directly to foreign, international, state, local, tribal, or private sector entities or individuals for the limited purpose of assisting NCTC in determining whether the U.S. person information constitutes terrorism information as provided for in the 2012 AGGs section IV.B.2. 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.

6. (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;***[31]

(U) As discussed in Section A *Periodic Reviews*, as of the end of the reporting period, there were no accesses to, or disseminations of, bulk datasets or significant portions of datasets containing U.S. Persons information (as permitted under Sections IV(B) and (C) of the 2012 AGGs.

(U) Should NCTC choose at some future point in time to consider engaging in bulk dissemination of U.S. Persons information (as permitted under Sections IV(B) and (C) of the 2012 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.

7. (U) ***An assessment of whether there is a need for enhanced safeguards, procedures, or oversight regarding the handling of United States person information or other sensitive information, or whether any other reasonable measures that should be taken to improve the handling of information;***[32]

(U) Enhanced Safeguards Assessment: Pursuant to Section III.C.3(e) of the 2012 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 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 U.S. Person that might result from improper use or disclosure of the data, and other relevant considerations.

(U) As was described in the previous report, NCTC has established a process to assess each Track 3 dataset anew for application of Enhanced Safeguards prior to signing new T&C documents for datasets under the 2012 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

[30] (U) Id., §VI.D.2(5)
[31] (U) Id., §VI.D.2(6)
[32] (U) Id., §VI.D.2(7)

makes recommendations to the D/NCTC regarding the appropriateness of enhanced safeguards.

(U) To aid this board, a Track 3 Enhanced Safeguards Matrix was 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 leading to 13 enhanced safeguard decisions specific to nine (9) Track 3 datasets on nine (9) occasions. Those recommendations were coordinated with both the ODNI General Counsel and the ODNI Civil Liberties Protection Officer prior to review and approval by D/NCTC:

- May 2013, one travel-related dataset; no additional enhanced safeguards other than those previously required by the data provider; and one immigration benefits-related dataset; three enhanced safeguard (ES 2[33], 3[34], 8[35])[36]

- August 2013, three international travel-related datasets, each with separate recommendations:
  - Dataset One - three enhanced safeguards (ES 2, 3, and 8);
  - Dataset 2 - no additional enhanced safeguards other than those previously required by the data provider; and
  - Dataset 3 has two (2) feeds of data: feed one - no additional enhanced safeguards other than those previously required by the data provider; feed two – six enhanced safeguards (ES 1[37], 2, 3, 5[38], 7[39], 8);

- August 2013, an international travel-related dataset; no enhanced safeguards were applied;

[33] (U) ES 2 requires advance coordination with NCTC Legal and the data provider prior to the dissemination on non-TI.
[34] (U) ES 3 requires special training regarding the use and handling of the dataset prior to granting access to the data.
[35] (U) ES 8 requires more frequent spot checks (no less frequently than every six months) of the ES 2 requirement for coordination of non-TI disseminations.
[36] (U) In the course of preparing this report, after the conclusion of the reporting period, NCTC Compliance discovered that this Enhanced Safeguard determination was not communicated to the current compliance regime during the transition from the former compliance regime. As a result, the identified Enhanced Safeguards for this dataset have not been audited. NCTC Compliance will document this as a compliance incident and begin auditing the identified Enhanced Safeguards in FY'16.
[37] (U) ES 1 requires additional role restricted access to the dataset determined in coordination with the data provider.
[38] (U) ES 5 requires limiting access to especially sensitive information within the dataset through the use of privacy enhancing technology such that the data is discoverable, but that additional approvals, including verification of a demonstrable need-to-know, are required before accessing the data.
[39] (U) ES 7 requires more frequent spot checks (no less frequently than every six months) of the ES 1 requirement for additional role restricted access to the dataset determined in coordination with the data provider.

- September 2013, an international travel-related dataset; no additional enhanced safeguards other than those previously required by the data provider;

- April 2014, a pilot project involving two immigration benefits-related datasets; three (3) enhanced safeguards (ES2, 3, 8) [40];

- May 2014, an immigration benefits-related dataset; three (3) enhanced safeguards (ES 2, 3, 8) [41];

- June 2014, another international travel-related dataset. Initially, the DAUG recommended, and the Director of NCTC agreed that no additional safeguards should be imposed other than those previously required by the data provider. However, upon further negotiations with the data provider, NCTC agreed to impose ES 2.

- July 2014, a sub-set of data protected data within seven (7) immigration-benefits and travel-related datasets , three (3) enhanced safeguards (ES2, 3, 8[42];

- December 2014; an international travel-related dataset was reconsidered due to the receipt of additional data fields; no additional enhanced safeguards imposed; new fields added to the dataset.

8. (U) ***A description of measures that NCTC has taken to comply with the requirements of section VI.C[43] with respect to its data processing systems;[44]***

(U) As detailed throughout this report, numerous efforts were undertaken during the reporting period to enhance NCTC's ability to monitor activity involving U.S. Person information and other sensitive information, while facilitating compliance with, and the auditing and reporting required by, the 2012 AGGs. Such activities included, but were 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 U.S. Person Track 3 data. Enhanced the detail of the information captured in the logs and closed any logging gaps discovered;
- (U) Audited a random sampling of all accesses to U.S. Person 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;

[40] (U) See footnote 36.
[41] (U) See footnote 36.
[42] (U) See footnote 36.
[43] (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.
[44] (U) Id., §VI.D.2(8)

- (U) Displayed 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;
- (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 AGGs and their role/responsibilities in upholding and complying with them.
- (U) Levied requirements on new IT development projects to facilitate ground-up development that includes the necessary safeguarding and auditing capabilities for AGGs compliance;

9. (U) ***A description of any material changes or improvements NCTC implemented, or is considering implementing, to improve compliance with these Guidelines;***[45]

(U) One of the most significant material changes NCTC implemented during this reporting period was a change to the frequency with which Baseline Safeguard audits were conducted. Our previous report stated that each Baseline Safeguard audit would be conducted each quarter. However, NCTC very quickly discovered that due to the complexity of conducting the audits and the systemic challenges presented within the audit processes as originally designed (further discussed below), quarterly auditing of all Baseline Safeguards was not possible. As described elsewhere in this report, the inability to quickly and easily identify individuals' organizational assignments introduced significant unanticipated manual research into current organizational assignments in order identify the appropriate supervisory personnel to verify the appropriateness of the personnel activities such as data access and the narrow tailoring of queries. As a result of this unanticipated manual aspect to the auditing, significant time delay was introduced that further hindered NCTC Compliance's ability to accurate audit the Baseline Safeguards. These factors taken together severely limit NCTC's ability to frequently run its audit cycle as they result in the need for large amounts of manual labor to conduct each audit cycle. As a result, in the first quarter of Fiscal Year 2014 (October – December 2013), NCTC transitioned to a schedule of staggered quarterly auditing with each safeguard being audited semi-annually. In accordance with this new schedule, Baselines Safeguards 1, 2, and 4 were to be audited in quarters 1 (Oct. – Dec.) and 3 (Apr. – June) of the fiscal year and Baseline Safeguard 3 was to be audited in fiscal year quarters 2 (Jan. – Mar.) and 4 (July – Sept.).

(U) Additional material changes and improvements have occurred within the Center throughout the reporting period which have had an immediate and positive impact on NCTC monitoring and compliance activities in support of the 2012 AGGs. Our previous report discussed one improvement made to the Data Catalog, namely the addition of a planned deletion date for both US and non-U.S. Person information, which facilitated awareness and compliance with deletion requirements specific to U.S. Person. Two additional enhancements to the Data Catalog were made during this reporting period. The Data Management Team (DMT) first scrubbed the Data Catalog to ensure that all information previously existing in the Access Database[46] had been successfully transferred to the Data Catalog. Shortly

[45] (U) Id., §VI.D.2(9)
[46] The Access Database preceded the Data Catalog.

thereafter, a change history was added to the Data Catalog so that all data changes could be logged, to include but not limited to the file receipt and delete dates.

(U) Our previous report also advised that during the 2012-2013 reporting period, NCTC began automating deletion scripts and tailoring the deletion scripts to be collection specific[47]. In addition, deletion scripts have also been changed to read "greater than or equal to" the required deletion date. Prior practice was to write the deletion script to only include the "greater than" date, resulting in records not being deleted on the scheduled deletion date (i.e. would be deleted one day after, or one day "greater than", the scheduled delete date).

(U) NCTC's previous report also noted an NCTC Mission Systems recommendation to establish a planned deletion date of seven days prior to the required deletion date for all data in NCTC's holdings. That recommendation was approved and was implemented as of 22 April 2013. The previous practice was to delete data on the required deletion date. If the deletion failed to occur, however, a compliance incident would result as the earliest date on which the error would be discovered would be the following day (i.e. one day after the required deletion date). The current practice of deleting data seven days prior to the required deletion date allows for the verification of the deletion and, in the event the deletion failed to occur, the ability to correct the error/delete the data within the permissible retention period.

(U) NCTC is also in the early stages of developing a web based tool to establish a "dashboard" to reflect the ongoing status of various hosts and services related to routine data processing. Initially, the dashboard will reflect the status of data ingestion; data extraction, transformation and loading (ETL) extraction; and exposure of each dataset to end users. Enhancements and additional capabilities will continue to be added once the baseline dashboard is functional.

(U) Additionally, as noted in the discussion of Baseline Safeguard 1 in Section II. B., *A general description of NCTC's compliance and audit processes,* above, effective FY15Q3 (Apr – June 2015), NCTC Compliance modified its audit processes in order to provide a more holistic view into privileged user access. Previously, the audit **selected at random 5%, but no more than 15, privilege user logons** from 7 servers with privilege user activity on the audit date. The 7 servers, with activity, are selected at random, via script, from all Track 3 servers with activity during the twenty four hour audit period. Beginning FY14Q3, per the direction of the Compliance Officer, the definition of a logon was further defined as any activity performed by a privileged user on the audited server within a 15 minute period. As a result of running the above audit, NCTC Compliance found that the current process was overly stringent and caused a loss of over 95% of privileged user activity. In most cases, a manager often reviewed only one (1) logon for a single user, when there may have been additional users with activity on the audited Track 3 servers.

(U) To present a more holistic view into privileged user accesses, NCTC Compliance modified the script to now select **at random up to 15 unique users** from each of the 7 servers selected for audit. The 7 servers continue to be selected at random, via script, from all Track 3 servers with activity during the audit period. The selection of 15 unique users is a significant change to the BSG 1 audit processes as it removed the previous limits of 5% of

[47] As previously reported, this accommodates the possibility that duplicate identifiers are used in different datasets

the privileged logons (i.e. user activity performed within a 15 minute interval) and refocused to provide up to 15 privileged users who accessed the servers on the given audit day.

(U) As described above, in the discussion of Baseline Safeguard 2 in Section II. B., *A general description of NCTC's compliance and audit processes,* during FY15, NCTC Compliance initiated a series of actions to develop solutions to the challenges of auditing BSG 2 which will be discussed in further detail below. First, NCTC Compliance created a new database, Beacon, for the tracking of compliance training and data access authorizations and removals. This database replaced a more decentralized tracking process with a one-stop repository that improved the effectiveness of tracking, auditing, and reporting on compliance training and data access, as well as gaining efficiency in the process. Additionally, NCTC Compliance undertook a manual effort to review and update the organizational affiliation of all U.S. Government personnel reflected within NCTC IT systems, including the VDE. Additional changes, including the review and updating of all contractor affiliations, will continue in FY16 and are further discussed below.

(U) **Planned Process Improvements:** While NCTC Compliance performed Baseline Safeguard audits with regular frequency, NCTC Compliance found that the audits emphasized the Center's inability to accurately and consistently identify individuals with access to Track 3 datasets in a timely manner. As a result, the data being audited was often stale by the time it was forwarded to the appropriate supervisor for verification making it difficult, if not impossible, for the supervisor to accurately assess the compliance due to the excessive delay between the action and the audit review date. These findings stem from the Center's lack of an automated tracking capability for personnel arrivals, departures, and reassignments. To remediate the difficulties in identifying and tracking down organization assignments of personnel, NCTC Compliance developed a combination of manual and automated processes, including regular updates as a first step towards identifying the assigned organization of personnel in the Center. Even with these small process improvements, NCTC Compliance has already reduced the number of individuals whose organizational assignment must be researched during the audit process. NCTC Compliance will continue to implement additional improvements during the next reporting period.

(U) NCTC Compliance audits have been in place since 2013 and as noted above in the section on Audit Findings and Shortcomings, NCTC has found numerous other areas where process improvements are necessary. To redesign, test, and implement these improvements, NCTC Compliance is reducing the frequency of periodic audits to once annually for the next reporting period covering Fiscal Year 2016 (1 October 2015 – 30 September 2016) in order to allow for the redesign, testing, and implementation of improved auditing processes. ODNI CLPO, NCTC CLPO, and NCTC Legal agree that implementation of process improvements is necessary and will improve audit accuracy while simultaneously reducing the burden on manual labor and decreasing human errors. NCTC Compliance continues to work closely with NCTC CLPO and NCTC Legal to identify the best means of improving auditing and compliance processes to meet the Center's AGGs compliance obligations.

(U) The planned improvements to NCTC's oversight and auditing processes are intended to set the stage for the implementation of fully-automated processes that in the future will continually monitor for non-compliant activity and provide alerts when such activity is detected. To reach this goal, further investment in the program is necessary. NCTC Compliance continues to work with NCTC Legal, NCTC CLPO, and NCTC Mission

Systems to advocate for and pursue the necessary funding. Ahead of such investments, NCTC Compliance has identified several improvements that can be made to greatly increase effectiveness in some areas.

(U) Baseline Safeguards 1 and 3.2 –Auditing to date has focused on logs that capture access activity to the various IT equipment involved in processing and storing data. Two issues encumber this approach to auditing:

- Machine-to-machine interactions and human-to-machine interactions are indistinguishable in the logs. This means that the routine machine processing of data to make it available to analysts looks the same as human-initiated changes to the data in the audit logs. Thus, it is extremely difficult to know whether a privileged user accessed a server, and even hard to know whether that user was authorized to do so and changed any data during their access.
- Privileged users have the ability to alter server logs further increasing the difficulty in identifying unauthorized changes and manipulations of the data.

(U) The long-term solution to address the above two issues will be to incorporate more robust logging and monitoring software in our IT systems. Such software has been mandated by ODNI for the entire Intelligence Community and NCTC anticipates employing it across its entire IT infrastructure in time. In the interim, NCTC Compliance anticipates instituting the following auditing process improvements:

- Improved documentation and auditing of privileged users with access to the database level on servers holding Track 3 data. This may include, further documenting and monitoring the process for granting and removing privileged user authority. This would better ensure that the number of privileged users is minimized and that as personnel change roles or depart NCTC their accesses are promptly removed.
- Documenting the automated computer scripts used to undertake the routine processing of data within the Center's IT systems, including the extract, transform, and load processing that ingests the data into NCTC databases and applications where it is exposed for analyst use. Documenting these scripts, will allow for simpler identification of anomalous scripts that may be indicative of unauthorized changes and manipulations of the data.

(U) Baseline Safeguards 2, 3.1 and 4 – NCTC's implementation of BSGs 2 and 3.1 focuses on the processes by which ends users of the data are authorized for data access (role-based access); their actual data access (log-on/log-off); and the review of queries to ensure they are narrowly tailored. As noted numerous times in this report, auditing has revealed that HR and contracting records fail to effectively track changes in personnel assignments—this includes departures from NCTC. This weakness introduces substantial manual labor into the overall audit process and the opportunity for unauthorized access to data.

(U) The long-term solution will be to employ a new generation of access and personnel management software. NCTC/ODSI is working with the ODNI-led IC IT Enterprise (IC ITE) program and its executive agent for access management to ensure our needs are met in this future tool set. In the short-term, NCTC Compliance has developed a set of automatic and manual processes that combined will update and maintain staffing records of NCTC staff and contract personnel and compare those updated records against data

access logs to identify any unauthorized accesses. Because this process will operate with substantially less labor, we anticipate that we will be able to increase the frequency with which we conduct audits. This will result in a more secure environment for data entrusted to the Center. Additionally, NCTC Compliance will be exploring technical capabilities that will facilitate more timely identification and review of analyst queries thereby improving managers' ability to assess compliance with the query standard.

(U) As noted above, NCTC Compliance, in consultation with DNI OGC, NCTC Legal, DNI CLPO, and NCTC CLPO, has determined that it is necessary to reducing the frequency with which all Baseline Safeguards will be audited by FY2016 (1 October 2015 – 30 September 2016) in order to design, test, and implement new audit procedures. The new audit procedures will be in full operation by 1 October 2016. We look forward to providing a detailed update on the new audit processes in our next report.

C. NCTC AG Guidelines Outreach & Transparency Measures

(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 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 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 U.S. Person data under the 2012 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 released and posted on its website the following documents:

- Memorandum of Understanding between FinCEN and NCTC (redacted);
- Overview of the Baseline Safeguard Protections Under NCTC's 2012 Attorney General Guidelines;
- Enhanced Safeguards Decision Matrix;
- NCTC Compliance Incident Procedures Regarding Data Handling (redacted);
- Overview of NCTC's Data Access as Authorized by the 2012 Attorney General Guidelines;
- NCTC's Annual Report on the Access, Retention, Use, and Dissemination of United States Person Information for the Period March 23, 2012 – March 21, 2013 (redacted);
- Memorandum of Agreement Between the Department of Homeland Security and National Counterterrorism Center Regarding Advance Passenger Information System (ADIS) Data (redacted);

(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.

Attachments:
1. (U) Annual Review of Track 3 Ingestion ([redacted]
2. (U) Classified Annex ([redacted]