

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~☐ (b)(2)
(b)(3)
(b)(6)

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
CIVIL LIBERTIES PROTECTION OFFICER
WASHINGTON, DC 20511

E/S #

MEMORANDUM FOR: The Honorable Jane Holl Lute
Deputy Secretary
Department of Homeland Security

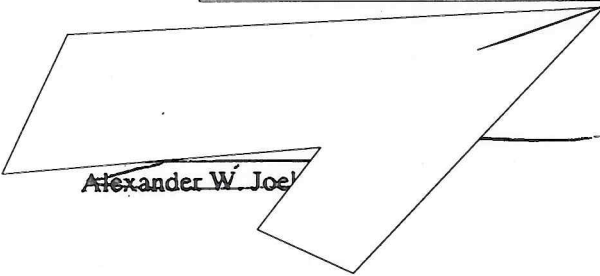
SUBJECT: (U) Review of Compliance Incident Involving Retention of Data
from DHS APIS Data by NCTC

REFERENCES: A. (U//~~FOUO~~) CLPO Compliance Incident Review Report
Incident Number 2010-Oct-01

(U//~~FOUO~~) Enclosed please find a copy of the review conducted by the ODNI's Civil Liberties and Privacy Office (CLPO) of the above-referenced compliance incident, which arose during October/November 2010.

(U//~~FOUO~~) The attached review sets forth the chronology of relevant events, summarizes CLPO's assessment of the incident, describes the corrective measures taken (in consultation with CLPO), and documents additional recommendations. CLPO concludes that the measures taken following the incident, coupled with CLPO's additional recommendations, adequately respond to the incident and its ramifications.

(U//~~FOUO~~) If you have any questions, please contact the Civil Liberties Protection Officer at



Alexander W. Joe

April 5, 2011
Date

Attachment:

1. (U//~~FOUO~~) CLPO Compliance Incident Review Report Incident Number 2010-Oct-01

cc: Marry Ellen Callahan, Chief Privacy Officer, Department of Homeland Security

UNCLASSIFIED when separated from Attachment.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

U//~~FOUO~~

**Office of Director of National Intelligence
Civil Liberties and Privacy Office
Compliance Incident Review Report**

Incident Number: 2010-Oct-001

Date of Incident: October 17, 2010 (through November 30, 2010)

I. Summary of Incident:

On November 29, 2010, NCTC discovered that it had retained information from the DHS APIS system beyond the agreed upon 30-day period. Once the error was discovered, the data was deleted within 24 hours, and the incident was reported by NCTC Director to DHS Deputy Secretary. The ODNI Civil Liberties and Privacy Office (CLPO) subsequently conducted a review of the incident and worked with NCTC to implement responsive measures.

II. Methodology:

CLPO conducted interviews of numerous NCTC personnel over the course of three months, including personnel within: a) NCTC's Missions Systems; b) NCTC's Directorate of Intelligence, Information Integration Group (IIG); and c) NCTC's Information Sharing Program and Policy Office (ISPPPO). CLPO also examined relevant documentation, and worked closely with relevant NCTC personnel on appropriate remediation efforts.

III. Chronology:

- September 2, 2010 – APIS data transmittal letter from DHS (communicating the 30-day deletion requirement for APIS data) arrives at the Office of the Director, NCTC) but is improperly routed.
- September 3, 2010- APIS historical data arrives at NCTC on 12 DVDs.
- September 17, 2010- NCTC receives the lookup/reference tables necessary for access and use of the APIS historical data. Based on the deletion requirements known at the time, the IIG's Chief established a deletion date of January 1, 2011.
- October 4, 2010 – APIS historical data is loaded onto NCTC systems for operational use.
- October 17, 2010 – Date for NCTC deletion of APIS historical data as contemplated by APIS transmittal letter (30 days from receipt of lookup/reference tables).
- October 30, 2010 – NCTC IIG's Chief first learns of the 30-day deletion requirement.
- October 30, 2010 – DHS changes the start date for calculating the 30-day retention period, from September 17, 2010 (date of data receipt) to October 4, 2010 (date of data load).
- November 29, 2010 – NCTC's IIG Chief formally becomes aware of NCTC's failure to comply with the APIS deletion requirement during a meeting with DHS and notifies DHS, NCTC Director.
- November 29, 2010- NCTC Legal sent an email to ODNI CLPO informing him of NCTC's

U//FOUO-

failure to comply with the APIS deletion requirement. (A representative from NCTC legal was present at the meeting where it was discovered that NCTC had failed to comply with the data deletion requirement.)

- November 30, 2010 - deletion of the past-due APIS data is completed.¹
- November 30, 2010 - NCTC calendar tool is set to flag deletion of APIS data on rolling 30-day basis.
- December 4, 2010 – the first of the rolling 30-day deletion activities is implemented, on schedule²

IV. Summary of ODNI/CLPO Assessment:

- At the time of this incident, NCTC had in place a comprehensive data management system that ordinarily would have tracked the deletion date for this data. However, that data management system did not account for the possibility of data arriving through non-standard processes, as occurred in this case.
- APIS data was secured through non-standard processes. This set the stage for the following:
 - The APIS data transmittal letter from DHS communicating the 30-day deletion requirement arrived at NCTC on September 2, 2010, prior to receipt of the data itself. Due to misrouting within NCTC, the letter was not provided to ISPPPO or IIG, or the Mission Systems' Data Management Team (which is responsible for calendaring action events, including deletion dates).
 - Although APIS historical data was delivered to NCTC on September 3, 2010, this data could not be processed, staged and utilized until NCTC received the associated lookup/reference tables, which were not delivered to NCTC until September 17th.
 - Because NCTC was not able to "review" the APIS data until receipt of the lookup/reference tables on September 17, 2010, the first APIS data deletion date -- had NCTC been aware of the requirement -- should have occurred on October 17, 2010. However, unaware of the DHS transmittal letter (and the 30-day deletion requirement), IIG's Chief established a deletion date of January 1, 2011, based upon early, preliminary negotiations with DHS for APIS data. The Data Management Team calendared the deletion activity for January 1, 2011.
 - Ordinarily, ISPPPO verifies the deletion requirements for data sets received, and drafts formal data handling instructions. Not having been involved in the APIS data acquisition process, however, and having not received the data transmittal letter from DHS, ISPPPO did not issue any data handling instructions in this case.
 - IIG's Chief learned of the 30-day deletion requirement for APIS data during a DHS-NCTC meeting on October 30, 2010. However, he failed to document or otherwise convey this requirement to the Data Management Team, and the January 1, 2011 calendar date for deletion of APIS data remained unchanged.

¹ Past due APIS datasets that were deleted included data received on September 3, 10, 17, 22, and 29, and October 6, 13, 19, and 26.

² Includes deletion of data received on November 5.

U//~~FOUO~~

- On November 29, 2010, at the next monthly meeting with DHS, the IIG Chief was alerted to this compliance issue when DHS asked whether NCTC had completed deletion of the first batch of APIS records (which should have been deleted on November 4, 2010). At this point, he immediately notified the DHS Chief Privacy Officer, the NCTC Director (who subsequently notified the DHS Deputy Secretary).
- Past-due deletions of APIS historical data and weekly updates were undertaken immediately, and completed on November 30, 2010. Additionally, the NCTC data calendar tool was set to flag APIS data for deletion on a rolling 30-day basis.

V. Summary of Corrective Measures Taken:

The following changes to NCTC's data management procedures have been implemented as a result of the incident:

- Internal clarification that ISPPPO is the only entity at NCTC authorized to enter into data acquisition arrangements.
 - Written guidelines have been issued and training conducted for all personnel at NCTC involved in the acquisition of data sets.
- All written data handling instructions will flow directly from the data provider to ISPPPO.
 - ISPPPO will examine incoming requirements provided by the data provider, as well as the description of the incoming data sets (to determine whether policy requirements require additional special handling instructions), and will memorialize its findings in written data handling (retention, use and deletion) instructions.
 - To ensure consistency, ISPPPO, in coordination with NCTC Legal, will review and compare data handling instructions against letters/MOUs/other requirements provided to NCTC by the data provider at the time of transmittal.
 - Where ISPPPO, in consultation with NCTC's Legal, determines that NCTC needs more specific instructions from the provider for purposes of drafting the data handling instructions, ISPPPO will contact the provider and obtain such instruction.
- Before data can be formally "ingested" by NCTC, it must be accompanied by official, written data handling instructions from ISPPPO.
 - Mission Systems, NCTC's only entry point for placing data into its data layer, have been provided with written guidance prohibiting the loading of data until they receive written data handling instructions from ISPPPO.
 - Staff approval at the Group Chief level is required to verify that the applicable ISPPPO data handling provisions are associated with the data set.
- Data flowing in through non-standard paths, or without written data handling instructions from ISPPPO, will be automatically referred to ISPPPO.
 - Those responsible for implementing access, use, retention and deletion instructions will no longer accept instructions from anyone except a representative from ISPPPO.
- Verbal changes to data handling instructions are not permitted.
 - All communications regarding dataset requirements must be in writing.
 - If verbal instructions are provided and communicated to data managers or ISPPPO, ISPPPO will follow up with the data provider to secure the instructions in writing.
- Override procedures will be developed to ensure that acquisition of data provided as part of an

U//FOUO

immediate mission need can be quickly ingested, but are also tracked and reviewed by ISPPPO.

- In such cases, a Group Chief must approve the loading of the data, at which time the Group Chief will review all data restrictions (provided by the data provider) and develop "interim operating instructions."
- Notification of this ingestion of data outside of the ordinary process will be sent to ISPPPO the next work day.
- The Data Management Team, which is responsible for cataloguing data and preparing it for action by NCTC technical teams, will then follow up with ISPPPO to begin development of written data handling instructions.

VI. CLPO Conclusions & Recommendations:

Having completed its review of the APIS compliance incident, CLPO concludes that NCTC has taken adequate remediation/preventative measures in response to the incident, including:

- proactively notifying DHS upon discovery of NCTC's failure to comply with DHS' deletion requirements
- notification of ODNI/CLPO within 24 hours of NCTC's discovery of the compliance incident
- deletion of the data within 24 hours of NCTC's discovery of its failure to comply with the DHS deletion requirements
- counseling of the IIG official responsible for the incident
- conducting an internal review, in conjunction with CLPO, to identify the specific missteps that led to the compliance incident in question and implementing specific operational and policy changes to address each issue highlighted (described in prior section)
- expediting establishment of a dedicated NCTC Civil Liberties and Privacy Officer

In addition to the foregoing, NCTC is developing appropriate documentation to incorporate and formalize the changes referenced above, and is reviewing other data holdings to verify the adequacy of documentation and procedures based on lessons learned from this incident. CLPO is working closely with NCTC on these efforts, as well as on efforts to identify and implement such other compliance measures as may be appropriate within the context of NCTC's data acquisition, ingestion, and management activities.

Finally, while not necessarily a contributing factor here, this review has highlighted the need for greater clarity regarding "activation" of the 30-day deletion period. Opinions of those interviewed varied; some believe the 30 days begin with the date of physical receipt of the data set, some cite the date of receipt of the lookup/reference tables, and some cite the date that the data is moved into the operational environment. Indeed, the APIS transmittal letter itself was ambiguous on this point, stating that "information will be reviewed within 30 calendar days," raising the question of whether the 30-day period begins before receipt of the lookup/reference tables, without which the data could not actually be "reviewed."

To avoid future misunderstandings, CLPO recommends that new or modified agreements explicitly specify the conditions precedent for initiating deletion activity and for calculating critical time periods.