(b)(1)
(b)(3)
(b)(6)

~~SECRET~~

ASSESSMENT OF COMPLIANCE INCIDENT

FROM: NCTC Legal
(Drafted by [redacted] Legal Counsel)

RE: Compliance Incident: Delayed Deletion of APIS Data

DATE: August 21, 2012

CC: NCTC's Civil Liberties and Privacy Officer

I. SUMMARY OF THE FACTS

(U//~~FOUO~~) The Advanced Passenger Information System (APIS) is a Department of Homeland Security (DHS) dataset shared with the National Counterterrorism Center (NCTC) pursuant to a Memorandum of Understanding between NCTC and DHS dated June 28, 2011. Section 5(B) of that MOU requires that NCTC process "all APIS Records within 180 calendar days of receipt from DHS to determine whether those records constitute terrorism information. No more than 180 calendar days from receipt, NCTC will purge all APIS Records that do not constitute terrorism information."

(~~S~~) In moving from a manual to an automated deletion system in mid-February 2012, an APIS look-up table that was designed to generate identities was inadvertently left off the deletion script. Thus, deletions from February 15 to May 14, 2012, for this single look-up table, did not occur until the script error was found on May 14, 2012. At that time, NCTC Mission Systems corrected the script error. On May 14, 2012, Mission Systems deleted the look-up table and modified internal processes to ensure further automated deletions consistently occur. On May 15, 2012, Mission Systems verified that the incident was not a security issue or breach of personally identifiable information, because the data was not visible to any user or tool.

(~~S~~) On May 22, 2012, Missions Systems informed the Information Sharing Program and Policy Office (ISPPO) of the incident; the same day, ISPPO reported by email to DHS the occurrence of the incident and the immediate remedial measures taken. For more details regarding the incident, please see the attached compliance incident review report form, submitted by Mission Systems on June 18, 2012 to NCTC Legal and NCTC's Civil Liberties and Privacy Officer.

II. ANALYSIS OF THE COMPLIANCE INCIDENT

A. Determination of whether this is a compliance incident under the 2008 Attorney General NCTC Guidelines and the 2011 MOU between DHS and NCTC

(~~S~~) This incident violated the 2008 Attorney General Guidelines implementing Executive Order 12333 as well as the 2011 MOU between DHS and NCTC. Under the Guidelines, NCTC

must "promptly remove" US Persons information that has not been deemed to be terrorism information. By NCTC policy, "promptly remove" has been interpreted to mean 180 days. This particular MOU specified the "prompt removal" requirement: in Section 5(B) of the MOU, non-terrorism information must be purged 180 days from time of receipt at NCTC. NCTC sought to apply the 180-day retention period to this dataset, but did not do so because of a deletion script error. In summary, the express terms of the MOU and NCTC policy were violated by not deleting the non-terrorism information with 180 days of receipt at NCTC. In addition, because the 2008 NCTC AG Guidelines have been interpreted via NCTC policy to require removal of data within 180 days, the Guidelines were also violated.

(S) No NCTC analysts or others viewed the dataset after the 180-day retention period had passed. Once the deletion error was discovered, that very same day Mission Systems deleted the data that had been held longer than 180 days. Ultimately, no US Persons data was accessible, viewed or misused, and DHS – whose data was at issue – was informed once the error was realized, and NCTC undertook remedial efforts to understand why there were flaws in the deletion script and to correct those flaws. According to the attached incident report, NCTC will make the following changes to data management procedures as a result of this incident:

- "The development teams will expand their testing to include peer reviews for deletion/retention integration. This will involve two or more developers performing additional tests and inspections prior to releases."
- "CTDL [Counterterrorism Data Layer] is also implementing random spot checks deletion/retention. The random spot checks will be conducted bi-weekly on one random dataset. This will involve a Systems Engineer working with the Database Administrators, Developers, and/or System Administrators."

B. This is not an "IOB-reportable" compliance incident

(U) The *Criteria on Thresholds for Reporting Intelligence Oversight Matters* state in relevant part:

- Intelligence activities are reportable if a reasonable person would believe they may be unlawful or contrary to an Executive Order or Presidential Directive;
- Violations of procedures and guidelines that heads of departments or Intelligence Community components have established to implement EO 12333 should be reported if such matters are of potential presidential interest or deemed appropriate for the Intelligence Oversight Board's (IOB's) review, *e.g.*, because they involve the apparent violation of substantive rights of individuals;
- "Significant or highly sensitive matters" should be reported to the IOB as appropriate, if they constitute intelligence activities or serious criminal activities by intelligence personnel that "could impugn the reputation or integrity of the IC, or otherwise call into question the propriety of intelligence activities."

(S) Based on the attached report, we do not believe that this compliance incident constitutes activity contrary to law, Executive Order or Presidential Directive. The violation of the 2008 NCTC AG Guidelines and the MOU between NCTC and DHS on the prompt deletion of non-

terrorism information data does not appear to be a "violation of the substantive rights of individuals." Instead, it was a delay in removal of data, and during the delay period, the data was not actually accessed, reviewed, or used. Therefore, there was no adverse impact on the rights of individuals, and as a consequence no need to report the matter to the IOB.

III. CONCLUSION: NCTC need not take any further action

(U//~~FOUO~~) NCTC recognizes that, even if this incident is not IOB-reportable, it is important that we adhere to commitments to delete data appropriately under the 2008 NCTC AG Guidelines and any MOU. To emphasize the point, we must ensure that deletion is done correctly going forward, and that if there is an "audit" of our practices by DHS or other providers, we have good documentation and processes to show how we make sure we are complete in our task, and how we have taken corrective measures to address prior incidents. That means that we document the incident, conduct a review, and make sure we identify the causes and have addressed those causes. The incident was documented in the attached compliance incident review report form, which also outlines the causes of the incident and ways to forestall such incidents in the future.

(U//~~FOUO~~) NCTC Legal and NCTC's Civil Liberties and Privacy Officer have reviewed that report and concluded that, for the following reasons, this compliance incident requires no further action:

- This incident was an error in tasking a script to remove certain data within the requisite 180-day timeframe (in other words, the intention was to adhere to the terms of the MOU, not to thwart them),
- Missions System personnel informed appropriate senior officials promptly once the error was discovered,
- Mission Systems deleted the non-terrorism APIS data the same day the script error was discovered,
- Mission Systems ascertained within one day that the data was not visible to any user or tool,
- Mission Systems fixed the incorrect script,
- Mission Systems undertook a review to determine what happened and fashioned new processes to forestall or detect such script errors in the future,
- ISPPO informed the data provider the same day ISPPO was made aware of the error, and
- Mission Systems wrote up the incident on the appropriate compliance incident review report form and submitted it timely to NCTC's Civil Liberties and Privacy Officer and NCTC Legal.

C05960965

~~SECRET~~

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

Incident Number: ____-___-___

Date of Incident: 15 February – 14 May, 2012

I. Summary of Incident:

During an internal compliance check on 14 May, 2012, NCTC/MS identified an isolated retention of APIS data past the data's deletion date. The data existed in a look-up table for use generating IDs. This data was in no way exposed to any users. The table did not contain the full APIS record but did contain PII. All other visible corresponding APIS data had been deleted on time per the agreement. NCTC receives approximately [redacted] records weekly. The number of records retained past the deletion date totaled [redacted] and were deleted immediately upon discovery. When APIS was changed from a manual deletion process to an automated deletion process, the look-up table in question was inadvertently left off the deletion script. Thus deletions from mid-February to 14 May, 2012 for this single look-up table had not occurred. This error has been corrected and internal MS processes have been modified to ensure it does not happen again. No other datasets are impacted by this. To reiterate, the data in question was not visible to any user or tool.

II. Methodology:

When the issue was identified, an immediate communication to MS/CTDL&S management was initiated. This kicked off information gathering sessions intended to identify the cause and process changes to prevent recurrence.

III. Chronology:

- 15 February, 2012 First automated deletion of APIS (lookup table not included)
- 14 May, 2012 DBA discovered data during internal compliance check – Data Deleted
- 15 May, 2012 MS/CTDL&S informed and investigation started
- 22 May, 2012 ISPPO informed in writing of incident, the cause, and the corrective actions to prevent happening again.
- Note - Based on the Twister controller job history, it was initially thought the duration extended from mid-March to 14 May.

IV. Summary of Assessment of Incident (measures/causes/actions that figured into incident):

- The Retention Deletion Management Service (RDMS) is developed and tested by a team of developers different than those who develop and test the scripts that actually interact with the data and perform the deletions.
- In this case there was a disconnect between the teams with respect to a true end to end test and validation of test results.

V. Summary of Corrective Measures Taken:

[redacted]

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

- The development teams will expand their testing to include peer reviews for deletion/retention integration. This will involve two or more developers performing additional tests and inspections prior to releases.
- CTDL is also implementing random spot checks deletion/retention. The random spot checks will be conducted bi-weekly on one random dataset. This will involve a Systems Engineer working with the Database Administrators, Developers, and/or System Administrators.

VI. CLPO Conclusions & Recommendations:

Having completed its review of the ____ compliance incident, CLPO concludes that NCTC has ___