

Brussels, 19.1.2017
SWD(2017) 20 final

COMMISSION STAFF WORKING DOCUMENT

**U.S. Response to the European Commission's Report on the Joint Review of the U.S. -
EU Passenger Name Record Agreement**

Accompanying the document

**REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND
THE COUNCIL**

**on the joint review of the implementation of the Agreement between the European
Union and the United States of America on the processing and transfer of passenger
name records to the United States Department of Homeland Security**

{COM(2017) 29 final}
{SWD(2017) 14 final}



Homeland
Security

August 31, 2016

Mr. Luigi Soreca
Director
Directorate D: Security
European Commission
Directorate-General Migration and Home Affairs
B-1049 Brussels, Belgium

Subject: *U.S. Department of Homeland Security (DHS) Response to the European Commission's Report on the Joint Review of the U.S. – EU Passenger Name Record Agreement*

Dear Mr. Soreca:

DHS appreciates the opportunity to comment on the European Commission's (EC) draft report to the European Parliament and the Council on the *Joint Review of the Implementation of the Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security*. We recognize and appreciate the substantial efforts made by the EU delegation before, during, and after the July 2015 Joint Review to objectively gather facts to make informed decisions regarding DHS's implementation of the terms of the Agreement.

The DHS team reviewed the draft report and submits this letter, per Article 23(3) of the Agreement, to be included as part of the EC's final report. DHS finds the EC draft report's conclusions to be largely consistent with the July 2015 U.S. – EU Joint Review and the Privacy Compliance Review conducted by the DHS Privacy Office as reflected in the June 2015 report¹, specifically as they relate to the overarching finding that DHS implements the Agreement in accordance with its terms.

As part of DHS's continued efforts to improve operations while respecting privacy, DHS agrees with the EC that good stewardship of PNR is an ongoing process. The technical and procedural auditing capabilities of DHS's system, while strong, continue to evolve and the Joint Review has been one of many contributors to this process. A number of changes have already been made or are in the process of being made that resolve many issues the EC report raises, such as improving statistical collections and parsing results that only pertain to EU PNR. Nonetheless, DHS would like to clarify and respond to certain areas of the report where context was lacking, particularly regarding 1) capping the number of authorized PNR users and 2) linking PNR to law enforcement events.

¹ https://www.dhs.gov/sites/default/files/publications/privacy_pcr_pnr_review_06262015.pdf

Areas in Need of Context

1. Capping the number of authorized PNR users

The draft EC report states that the “growing number of individuals with access to [PNR] is concerning,” yet the report describes the rigorous process authorized personnel undergo to receive and retain access to PNR. This process includes mandatory training, supervisory approval, and automated oversight, in addition to twice-yearly audits of all user access accounts to confirm the user still has a “need to know.” Indeed, the EC recommendation states that “DHS should restrict the number of officers with access to PNR to those having a strict need to know,” which is the exact benchmark DHS requires. However, DHS believes that to “restrict” the number of users based on criteria other than mission requirements and “need to know” is both unnecessary under the Agreement and does not improve individual privacy. In fact, reducing the number of authorized users to meet the Commission’s assessment would likely have exactly the opposite effect by reducing an officer’s access to information that is relevant and necessary to make an effective operational decision. The number of authorized users will fluctuate based on DHS mission needs and the current threat environment. Regardless of this number, however, technical and organizational oversight of all users’ access remains in place wherein after three Joint Reviews there have been no findings of misuse of PNR nor any privacy incidents.

Managerial and technical controls within the system also limit authorized users’ access to PNR at different points. For example, authorized users that wish to use depersonalized PNR must seek and obtain supervisory approval to do so and then only have access to that PNR for a limited amount of time. There is approximately one supervisor for every 12 authorized users, allowing for adequate oversight.

Based on this additional information, DHS respectfully requests that the recommendation to restrict the number of officers with access to PNR be removed from this report.

2. Linking PNR to Law Enforcement Events

The June 2015 DHS Privacy Compliance Review noted that “[d]uring the course of this review, the DHS Privacy Office found that there may be a high percentage of PNRs that are inaccurately linked to a law enforcement event and therefore not depersonalized after six months. CBP is reviewing the process to link PNR to a law enforcement event and assessing its law enforcement functionality and controls.” Since that time, CBP has carefully reviewed all PNR linked to law enforcement events and determined that the linking itself is not inaccurate.

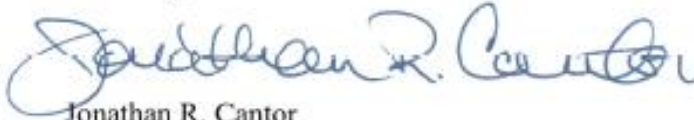
While the linking was found to be accurate, how we effectively use PNR in the current threat environment given CBP’s law enforcement authorities has caused CBP to work toward amending the criteria when linking PNR.

DHS believes that over the past year it has effectively “investigated” any “possible inaccurate linking of PNR to law enforcement events” and found the linking to be accurate

and in compliance with the terms of the Agreement. DHS is taking steps to amend its criteria to link PNR to law enforcement events to ensure DHS mission requirements are met while respecting data retention limits.

Thank you again for the opportunity to comment on the report. Should you have any questions or concerns about this letter, please contact me at 1-202-343-1717.

Sincerely,

A handwritten signature in blue ink, appearing to read "Jonathan R. Cantor". The signature is fluid and cursive, with a large initial "J" and a stylized "C" at the end.

Jonathan R. Cantor
Acting Chief Privacy Officer
U.S. Department of Homeland Security