EUROPEAN
COMMISSION

Brussels, 19.1.2017
SWD(2017) 14 final

COMMISSION STAFF WORKING DOCUMENT

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

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) 20 final}

COMMISSION STAFF WORKING DOCUMENT
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

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

Table of Contents

1. BACKGROUND AND PROCEDURAL ASPECTS OF THE JOINT REVIEW

Following the terrorist attacks on 11 September 2001, the United States (US) enacted a statute[1] and accompanying regulations[2], requiring all air carriers operating passenger flights to and from the US to provide access to certain Passenger Name Records (PNR) information to US Customs and Border Protection (CBP) – a component of the US Department of Homeland Security (DHS). In June 2002 the Commission informed the US authorities that these requirements could conflict with European and Member States' legislation on data protection which imposes conditions on the transfer of personal data to third countries.

As a result, the EU and the US entered into negotiations aimed at reaching agreement on sharing PNR data while securing an adequate level of data protection. The current Agreement between the EU and the US on the use and transfer of passenger name records to DHS[3] (hereafter the "Agreement" or "PNR Agreement") entered into force on 1 July 2012, replacing the previous one from 2007[4]. To avoid repetition about the background of these PNR Agreements, reference is made to the reports of the joint reviews carried out in 2006, 2010 and 2013.[5]

According to Article 23(1) of the Agreement, the Parties shall jointly review the implementation of the Agreement one year after its entry into force and regularly thereafter as jointly agreed. The first joint review of the Agreement was carried out in Washington one year after its entry into force[6] on 8 and 9 July 2013. In keeping with Article 23(1) the next joint EU-US review took place 1 and 2 July 2015, covering the period 10 July 2013- 5 May 2015. Under the terms of Article 23(2), the EU was represented by the European Commission, and the US was represented by DHS. The EU team also included two external experts; a data protection expert from the French data protection authority and a senior policy advisor from the UK Home Office. A representative from the Delegation of the European Union to the US was also part of the EU review team.

The methodology for the 2015 joint review exercise followed the same format as the review in 2013:

- The EU team was composed of 3 Commission officials, 2 external experts and a representative from the EU Delegation to the US.

---

1 Aviation and Transportation Security Act (ATSA), November 2001.

2 US Regulation 19 CFR 122.49d on PNR information.

3 OJ L 215/5, 11.08.2012.

4 OJ L 204/18, 04.08.2007.

5 Commission staff working paper on the joint review of the implementation by the U.S. Bureau of Customs and Border Protection of the Undertakings set out in Commission Decision 2004/535/EC of 14 May 2004, 20-21 September 2005, Redacted version, 12.12.2005. Reports 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 Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS), 8-9 February 2010, Brussels, 7.4.2010 and 8-9 July 2013, Brussels, 27.11.2013.

6 The agreement commenced on 1 July 2012.

- The Commission sent a questionnaire to DHS on 8 May 2015 in advance of the joint review. The questionnaire contained specific questions in relation to the implementation of the Agreement by DHS. DHS provided written replies to the questionnaire on 12 June 2015.
- The Commission also contacted all Member States to determine whether they had any contact with the US regarding PNR.
- The EU team was granted access to DHS premises and visited the DHS National Targeting Center (NTC).
- The EU team was given the opportunity to watch the targeting centre in operation.
- The EU team was given the opportunity to engage directly with DHS personnel responsible for the PNR program, including targeting and analytical staff that have access to and use PNR.
- The replies to the questionnaire were discussed in detail with DHS. The EU team also had the opportunity and the time to raise further questions to DHS officials and address all the various parameters of the Agreement.
- At the request of DHS, all members of the EU team signed a non-disclosure agreement as a condition for their participation in this review exercise. This exposes members of the EU team to criminal and/or civil sanctions for any breaches.
- DHS had the opportunity to ask questions to the EU team about the status of the EU PNR Directive and the discussions on PNR with other third countries.
- The DHS Privacy Office is responsible for monitoring the compliance of DHS with privacy and data protection legislation and oversees all handling of personal data by DHS. In preparation of the joint review exercise, the DHS Privacy Office prepared its own report on the use and transfer of PNR between the EU and the US. The DHS Privacy Office published its report on 26 June 2015.[7] Unfortunately this did not provide the EU team with enough time to analyse the report in full before the review on 1-2 July. However, the EU team subsequently analysed the Privacy Office report and asked follow-up questions which have assisted with the completion of the present report.
- For the preparation of this report, the EU team used information contained in the written replies that DHS provided to the EU questionnaire, information obtained from its discussions with DHS personnel, information contained in the aforementioned DHS Privacy Office report, as well as information contained in other publicly available DHS documents.

Due to the sensitive nature of the PNR program, there were limitations on the provision of some internal operational documents. During the meeting on 1-2 July 2015 each member of the EU team received a copy of the Management Directive for PNR approved by the Deputy Commissioner of US CBP on the use and disclosure of PNR. The Management Directive outlines the use, handling, and disclosure of PNR and provides a framework for granting

[7] Privacy Compliance Review - "Report on the use and transfer of passenger name records between the European Union and the United States", DHS Privacy Office, June 26, 2015. http://www.dhs.gov/sites/default/files/publications/privacy_pcr_pnr_review_06262015.pdf.

access to PNR to authorised personnel within DHS and for sharing PNR with DHS's domestic and international partners.

Before, during, and after the review the dialogue between the EU team and DHS has been positive, open and constructive, and DHS responded to all the questions raised. As with the joint review in 2013, this joint review allowed discussion on whether the Agreement serves its purpose and contributes to the fight against terrorism and serious crime.

The Commission would like to acknowledge the good cooperation of all DHS and other US personnel and express its gratitude for the way in which the questions by the review team have been responded to. The Commission also acknowledges the professional and constructive assistance it received from the two external experts who participated as part of the EU team.

Finally, the procedure for the issuance of this report was agreed with the US team and followed the procedure of the 2013 joint review report. The EU team prepared a draft report, which was sent to DHS, providing them with the opportunity to identify and comment on any inaccuracies or information that could not be disclosed to public audiences.

This report of the joint review has been written by the Commission, and is not a joint report of the EU and US. This report has been reviewed by the two external experts who participated as part of the EU team; a data protection expert and a senior policy advisor on PNR.

2. RECOMMENDATIONS FROM THE 2013 REVIEW

The 2015 joint review assessed whether DHS had implemented the recommendations made by the EU delegation during the previous joint review in 2013. Many improvements have been made but there are still recommendations from 2013 on which work is ongoing. The detailed updates below provide further information. In summary, positive progress has been made.

2.1 Retention of data (Article 8):

Recommendation from the 2013 Joint Review: the six month period referred to in Article 8(1) should start from the day the PNR is loaded in the US Automated Targeting System (ATS) (the so-called 'ATS load date') which is the first day the data is stored in ATS, instead of the current practice which delays the six month period until the last update of the PNR in the ATS. This recommendation was made to ensure that data was 'masked out' [8] as soon as possible.

[8] To depersonalise means to render those data elements that could serve to directly identify the data subject invisible to a user. The US uses 'depersonlise' to refer to the automatic 'masking out' of PNR data when it is received. The EU uses 'masking out' and therefore this wording is used throughout the report.

Progress: **Completed**.
As recommended, the US has programmed the PNR system to automatically mask out PNR not connected to a law enforcement case six months from the date it is first stored.

2.2 Method of PNR transmission (Article 15):
Recommendation from the 2013 Joint Review: Particular attention should be given to use of the ad hoc "pull" method. It was recommended to DHS, in addition to its current logging of ad hoc "pulls", that better records of the reasons why the ad hoc "pull" method are applied in each case DHS uses this method would allow for a better assessment of the proportionality and a more effective auditing tool. In this respect it would be welcomed if the discussions in WCO/ICAO/IATA[9] on a common PNRGOV[10] "push" standard for the transfer of PNR data by the air carriers to the State authorities also would lead to a common standard for ad hoc "push"[11].

Progress: Improvements made, ongoing.
At the time of the 2015 review, 50 EU carriers were pushing PNR to the US and data was pulled from 4 carriers. This contrasts with 32 EU carriers pushing PNR, 15 of which data was pulled from at the time of the 2013 joint review. This demonstrates that progress has been made, but the target of Article 15(4) - that all airlines should push data after two years of the agreement entering into force - was not met.

Better records have been maintained regarding why the "pull" method has been used. All pulls were recorded for three main reasons: the carrier not providing ("pushing") the data (including hardware or software issues with the carrier), an unforeseen schedule change or unanticipated stop in the US and occasions when additional pulls were conducted by CBP officers where time sensitivities required an immediate refresh of information. Between June 2013 and May 2015, 531,823 additional pulls were undertaken by CBP officers. To set this in context, in 2011, 0.72% of all PNR was pulled, in 2012, 0.3%, 2013, 0.19% and 2014, 0.34%.

---

9 WCO – World Customs Organisation; ICAO – International Civil Aviation Organisation; IATA – International Air Transport Association.

10 https://www.iata.org/iata/passenger-data-toolkit/assets/doc_library/04-pnr/New%20Doc%209944%201st%20Edition%20PNR.pdf.

11 The "ad-hoc pull" of PNR may take place when, for technical reasons a carrier is unable to "push" data; when because of a specific, urgent threat there is a need to "pull" data between or after a "push" of data, or when a flight is unexpectedly diverted to the US because, for example, of a technical problem with the aircraft or weather conditions. The recommendation made in the 2013 Joint Review identified a need for an international technical standard for the "ad-hoc push" of PNR from a carrier in those exceptional circumstances when a necessary requirement for data arises outside of the expected "push" of data.

2.3 Police, law enforcement and judicial cooperation (Article 18)[12]:

Recommendation from the 2013 Joint Review: The EU team welcomed the DHS Privacy Office recommendation to improve the procedure aimed at notifying Member States when the sharing of EU PNR data between DHS and third countries occurs.

The EU team noticed that the level of law enforcement cooperation between the US and the EU when sharing advance traveller information required more attention. DHS was requested to respect its commitment to ensure reciprocity and proactively share individual PNRs and analytical information flowing from PNR with Member States and where appropriate with Europol and Eurojust.

Progress: Improvements made, ongoing.

Additionally, since July 2014 there is a CBP Officer posted to Europol as a liaison officer whose role is to exchange law enforcement information with Europol partners (including Member States), with a focus on disrupting terrorist travel. On a regular basis the liaison officer reviews reports on high-risk passengers who were identified through advance targeting, including through PNR. When the liaison officer identifies a targeted passenger with a nexus to a Member State, he shares the information in the report with the Member State's representatives. From October 2014 to June 2015, the DHS liaison shared the names of 122 persons suspected of being involved in terrorism with Europol and the relevant Member States. Under an existing written arrangement, DHS has shared PNR with the Border Force of the UK; one PNR for terrorism purposes and one PNR for transnational crime purposes.

2.4 Redress – transparency on redress mechanisms (Article 13):

Recommendation from the 2013 Joint Review: During the 2013 review, the EU team acknowledged the complex interaction between the different programs using PNR; CBP to make accurate, comprehensive decisions about which passengers require additional inspection at the port of entry based and also assisting the work of the Immigration Advisory Program (IAP) and the Regional Carriers Liaison Group Program (RCLG) where necessary within the scope of the Agreement[13]. The EU team saw a need to recommend more transparency on the possible interrelation of various programs and in particular on the redress mechanisms available under US law. Such transparency would allow passengers who are not US citizens or legal residents to challenge DHS decisions related to the use of PNR, in particular when the use of such data has led to a decision to recommend the denial of boarding by carriers.

Progress: Improvements made, ongoing.

It is positive that DHS Traveller Redress Inquiry Program (TRIP) is the single point of contact for the public. However, no enquiries related to the use of PNR or applications for judicial review have been received which could suggest a lack of awareness of this provision. DHS continues to review and update their public facing guidance. For example, the DHS Privacy

---

12 This recommendation also concerns Article 17 – Onward Transfer.

13 Commission Staff Working Paper 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, 8-9 July 2013.

Office advised that in response to this recommendation, DHS sent a communication to every US Embassy within the EU to ensure additional language (if not already present) was added to the travel portion of their websites.

However, in the interest of transparency, the US should continue to review all necessary means to ensure that all passengers regardless of their origin are made aware of the redress mechanisms available under US law. In 2015 the DHS Privacy Office carried out a Privacy Compliance Review (PCR)[14] of the Agreement. The report, published on 26 June 2015, recommended that CBP (the department within DHS responsible for processing PNR) should create a way to determine if / how requests for access to or redress involving PNR were received from EU citizens or residents to enable the DHS Privacy Office to better report on categories of people resorting to DHS TRIP. This is welcomed and seen as a positive step by the EU team.

3. OUTCOME OF THE JOINT REVIEW

The EU-US joint review took place in Washington, DC on July 1-2, 2015 and was hosted by the Privacy Office of the DHS. DHS, and specifically US CBP, is responsible for collecting and processing PNR under the Agreement.

Over the course of the two day review, DHS gave a series of presentations to explain how it has implemented the Agreement. Presentations included:

- CBP targeting methodologies
- PNR use in DHS programmes
- PNR oversight - role of the Chief Privacy Officer
- Data Framework – inclusion of PNR
- Receipt of PNR
- PNR data handling and sharing
- PNR access
- Rectification and redress
- PNR retention
- US privacy legislation.

In addition, the EU team visited the National Targeting Center (NTC) and were able to see where the PNR data is processed.

With regard to implementation, **the overall judgment of this report is that DHS continues to comply with the conditions set out within the Agreement**. This is explained in more detail in the main findings below.

[14] The Privacy Compliance Review - "Report on the use and transfer of passenger name records between the European Union and the United States", DHS Privacy Office, June 26, 2015.

3.1. Main findings

3.1.1 Scope (Article 2) - The carriers and data types covered by the Agreement.

DHS outlined the content of the 19 PNR data elements it processes (these are listed in the Annex to the Agreement) and confirmed that all of the data types are necessary to target serious crime and terrorism.

The Agreement applies to passenger flights between the US and the EU. In response to the questionnaire completed in advance of the review meeting (a copy of the questionnaire is included as an Annex to this report), DHS explained that based on flight numbers and airport codes, the targeting system automatically filters out and discards PNR for journeys that do not arrive in or depart from the US (non-US nexus PNR). However, designated system users may initiate a manual override function to analyse PNR that has been inadvertently identified as non-US nexus PNR. This mechanism is audited by DHS Privacy Office and is subject to random testing and analysis. Between July 2013 and May 2015 there were 1571 overrides to this mechanism from 290 different users (71.4 per month). This compares with an average of 21.3 per month from the previous review. Additional details of why these overrides occurred should be recorded to better understand the reasons for the increase. It would be useful for all such figures to be recorded on a regular (e.g. monthly) basis to allow for direct comparisons with previous results.

DHS informed that an enhanced oversight process is in place to ensure that the US can analyse each of the overrides when they occur to confirm their necessity. This supervision is important and between June 2013 and February 2015 (the majority of this review period), five warnings were issued to authorised users of PNR who accessed non-US nexus PNR, two of which were EU related. These appear to have been accidental but the oversight function permits the revocation of an officer's access to PNR if appropriate. Again, records of why each override occurred would assist in understanding the reasons behind the increase in overrides.

DHS applies the same level of data protection required by the Agreement for all PNR (including the processing of PNR data not collected under the Agreement) it acquires and processes. This ensures that all PNR collected from flights between the EU and US is protected. It also satisfies the requirements of Article 2(3) of the Agreement; that the Agreement covers carriers incorporated or storing data in the EU and operating flights to or from the US This is a positive effect of the Agreement and has raised the standard of data protection for all PNR collected by the US.

During the review, the US stated that in 2016 it plans to co-locate the passenger and cargo targeting centres. DHS confirmed that this move to co-locate the two teams would not result in an increased access to passenger PNR data.

Conclusion: The use of the override mechanism is subject to a number of conditions and while the number of overrides has increased during this review period, each override is still

subject to oversight. However, more information is required to account for the increase in the number of overrides and detailed records should be kept to ensure this can be monitored and reviewed. It is positive to see the US applying the same stringent data protection requirements of the Agreement to all PNR it acquires and processes.

Recommendations:

1) DHS should record detailed reasons of why overrides have been used to better understand why they occur.

2) DHS should ensure that all facts and figures provided for subsequent reviews relate to the same time periods and solely to PNR which falls under the scope of this Agreement. This will provide a clearer basis for comparison.

3.1.2 Provision of PNR (Article 3) – How the data is transferred and by whom.

During privacy compliance reviews, CBP provided the DHS Privacy Office with PNR from randomly selected dates. These PNR were analysed to determine whether any data beyond the 19 PNR data elements listed in the Annex to the Agreement were there. The Privacy Office found no additional data was present. The June 2015 DHS Privacy Compliance Review explains that in October 2014, it was found that users of a DHS mobile application were able to see unblocked sensitive codes and terms in PNR when undertaking certain queries. Once identified, DHS took immediate corrective action to filter out sensitive PNR codes and terms from displaying in the mobile application and produced a fix to prevent this from occurring again.

Conclusion: DHS continues to filter out any elements of PNR which are outside the 19 data elements listed in the Annex to the Agreement. It is positive that corrective action was taken immediately to resolve the issue with the mobile application.

3.1.3 Use of PNR (Article 4) – How the data covered by this Agreement may be used.

DHS explained the three main uses of PNR: 1) identifying connections between travellers through PNR, 2) list based searches and 3) scenario or rules based targeting developed through a process of risk assessment against several independent risk indicators. PNR is one of several sources of information for advanced screening of travellers; others include visa applications, the Electronic System for Travel Authorization (ESTA) and Advance Passenger Information (API). During the review, DHS provided statistics which showed that CBP recommended to the carriers that they not board[15] approximately 3300 travellers in 2014 based in part on its risk assessments, which include the results from PNR targeting rules. The reasons for these recommendations primarily include bases for inadmissibility, such as previous criminal convictions, national security concerns and previous overstay. DHS explained the various programs in place to actively assess the risk of air travellers before

[15] CBP Officers provide no-board recommendations to air carriers when individuals bound for the United States may pose a security threat or may otherwise be inadmissible.

arrival to the US, the main being the Immigration Advisory Program (IAP) and the Regional Carrier Liaison Group (RCLG).

DHS advised that under an interim solution[16] to address the current foreign fighter threat, all PNR data is being copied to a classified network, with increased security and further limited user access. This is to allow the PNR to be processed against classified information. The classified database is used exclusively for counter-terrorism purposes. Whilst this change should be acknowledged by the review, it does not appear to affect the Agreement as processing the data for counter-terrorism purposes falls within the scope. The data protection safeguards for the interim solution adhere to the limitations of the Agreement, and how these compare with the automated privacy protections of the standard DHS data framework model and the mitigation for related privacy risks are described in the DHS Privacy Impact Assessment of 15 April 2015[17]. The classified network can only be accessed by a more limited number of staff.

Conclusion: The US continues to use PNR in a way which is consistent with the Agreement. By using PNR in the three main methods of analysis outlined above, maximum value can be obtained from the data for law enforcement purposes.

3.1.4 Data security (Article 5) – Safeguards applicable to the use of PNR

DHS confirmed that there had not been any significant privacy incidents under Article 5 involving the PNR of an EU citizen. No EU authority had therefore to be informed under Article 5(4) of the Agreement.

All access to PNR is logged. A specific instrument (the CBP PNR Directive, updated June 2013) on the use and disclosure of PNR is in place to ensure the appropriate handling and disclosure of PNR maintained in the system. It also provides a framework for granting access to PNR to authorised personnel within DHS and for sharing PNR with DHS's domestic and international partners. Only authorised personnel within DHS have access to PNR and all user access accounts are audited biannually. Warning banners and automated email alerts flag any overrides or use of sensitive data. Five warnings have been issued to officers during this reporting period for erroneously accessing data without a US-nexus. All data within the system is automatically masked and retained according to the data retention periods stipulated in the Agreement. A system security plan was completed and approved by CBP on January 31 2014; this will be reviewed in three years.

---

16 The Privacy Compliance Review - "Report on the use and transfer of passenger name records between the European Union and the United States", DHS Privacy Office, June 26, 2015, states in a footnote on page 11 that 'the interim solution will only continue until the standard model of the Data Framework is capable of meeting the mission need. DHS remains committed to the standard model of the Data Framework for meeting DHS's mission needs in the long-term and the Department will revert to the standard model once the technical capabilities are available.'

17 http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhswide-dataframework-april2015.pdf

More than 14,000 users have access to view PNR in the Automated Targeting System's active database. This compares with 46,000 individuals who have access to API. Approximately 1200 of users with access to PNR are supervisors. All personnel are vetted and security cleared to have access to the data. The EU team repeatedly questioned the higher number of those with access to PNR; particularly as this represented a substantial increase to 2013 when approximately 12,000 had access to the data. DHS stated that the number of authorised users will fluctuate based on DHS mission needs and the current threat environment; however technical and organisational oversight of all users' access remains in place including each user's level of access being validated twice per year by supervisory and management review. DHS advised that not all of the 14,000 were given all levels of access (i.e., active, depersonalised and dormant status) to the data and access to PNR continues to be limited to those personnel with a confirmed need-to-know.

Conclusion: The CBP PNR Directive continues to accurately outline the conditions set by the Agreement. In accordance with the Agreement, DHS maintains strict user access control and each user's level of access is validated twice per year to ensure it is necessary. However, it is noted that five warnings have been issued when PNR without a US-nexus was incorrectly accessed (see 3.1.1). The growing number of individuals with access to the system is also concerning.

Recommendation:
3) DHS should restrict the number of officers with access to PNR to those having a strict need to know.

3.1.5 Sensitive data (Article 6) – Definition and handling of such information

DHS confirmed that certain codes and terms for sensitive data which may appear in PNR are blocked from view in the system and any sensitive data identified is deleted after 30 days. A list of these codes and terms was provided to the Commission. DHS confirmed that this list remains valid. DHS explained its procedures for accessing sensitive data. In exceptional cases where the life of an individual could be imperilled or seriously impaired, users with a supervisory access role can select a user to grant access to sensitive data. The system only allows a DHS user to access sensitive data once CBP's Deputy Commissioner has granted such access. Every morning the managers at the targeting centre receive an email notification informing whether a DHS user has accessed sensitive data. DHS told the EU team that no sensitive data has been accessed since the Agreement entered into force. If a DHS user accesses sensitive data of an EU citizen, DHS has to inform the Commission within 48 hours as stated in the Agreement. However, this procedure has never been used as no sensitive data has been accessed. DHS clarified that the sharing of PNR with the US Centers for Disease Control and Prevention included no sensitive data.

Conclusion: CBP records indicate that no sensitive data has been accessed using this method during the period of this review. For this reason DHS cannot provide the EU with any information about the performance of the reporting mechanism for overseeing such

exceptional access and use. It is positive that under DHS rules, DHS will provide notice to the Commission within 48 hours should sensitive data be accessed by DHS staff.

Recommendation:
4) DHS should regularly review the list of sensitive data codes and terms to ensure all sensitive information is being identified and automatically blocked by the system. Any changes to the list should be shared with the Commission.

3.1.6 Automated individual decisions (Article 7) – The need for manual intervention
DHS confirmed that no decisions are taken based solely on the automated processing of PNR. A CBP officer always takes the final decision of whether to submit a passenger to additional screening at the border.

Conclusion: This is in accordance with the Agreement.

3.1.7 Retention of data (Article 8) – How long data can be retained and in what format
As recommended in the 2013 Joint Review Report, the US programmed its system to automatically mask out PNR not connected to a law enforcement case six months from the time it entered the system, its "load date".

The DHS Privacy Office informed the EU team that it had found that DHS may have inaccurately linked a high number of PNR to law enforcement events. Consequently, these PNR were not masked out after six months. This finding was confirmed in the report on the use and transfer of PNR records between the EU and the US published by the DHS Privacy Office on 26 June 2015. The EU team asked DHS to further investigate the reasons for this presumed inaccurate linking of PNR with law enforcement events.

The June 2015 DHS privacy report also confirmed an increase in the number of PNR that DHS unmasked. PNR remains unmasked within the system for 24 hours after which it becomes masked out again. Following the Commission's recommendation in the 2013 Joint Review Report, a DHS user must now justify why PNR is unmasked. The EU team welcomed that the DHS had followed this recommendation.

Lastly, DHS informed that it is preparing the dormant database to store PNR of 5 years and older as foreseen under article 8(3) of the Agreement. The dormant database will become active on 1 July 2017.

Conclusion: DHS uses automated processes to mask out PNR. This process is compliant with Article 8 of the Agreement. However, the number of PNR linked to law enforcement events (and thus not subject to such masking out) is high. Further investigation regarding the possible inaccurate linking of PNR to law enforcement events is required to understand why it is high.

Recommendations:

5) DHS should further investigate why a high number of PNR may have been inaccurately linked to law enforcement events and to take appropriate remedial action as necessary.

6) DHS should regularly review the linking of PNR to law enforcement events to ensure PNR no longer required can be deleted as soon as possible.

3.1.8 Non-discrimination (Article 9) – How safeguards must be applied to all data

DHS provided the EU team with copies of the CBP PNR Directive, which all DHS users must comply with when analysing PNR. The CBP PNR Directive contains specific provisions on non-discrimination. As the CBP PNR Directive is a restricted document, the EU team was only given limited time to read it and had to return it shortly afterwards. However, the team agreed that from what they saw, the Directive seemed to be in line with Agreement. The June 2015 DHS Privacy Office report also states that to ensure that the Department does not use PNR to illegally discriminate against individuals, quarterly reviews of all targeting rules are undertaken with the DHS Office for Civil Rights and Civil Liberties and the DHS Office of the General Counsel.

Conclusion: In compliance with Article 9, high levels of safeguards are applied to PNR to ensure the non-discrimination of individuals. In particular, the quarterly review of all targeting rules with the Office for Civil Rights and Civil Liberties is welcomed. The EU team review of the CBP Directive appeared to show that it supported the agreement but a more thorough examination of the Directive is required.

3.1.9 Transparency (Article 10) – Public information regarding the use of the data

The 2015 DHS Privacy report highlights the mechanisms for providing the public with information, through US Embassies in the EU, on how DHS uses PNR and opportunities for individuals to seek access to information and to seek redress. The DHS Privacy Office report also suggests further increasing awareness by launching information activities through the Embassies of Member States. The Agreement is published on the DHS website, along with copies of previous joint review reports. DHS/CBP's 'procedures for access, correction or rectification and redress for PNR', along with updated contact information are also published online. DHS has also communicated with air carriers and provided appropriate language regarding transparency to include in their contracts of carriage.

Conclusion: In accordance with Article 10 of the Agreement, there is a wide range of information available online regarding how DHS handles PNR, including the most recent DHS Privacy Office Report. DHS should strive to be as transparent as possible and continue to ensure that this information is updated.

3.1.10 Access, correction or rectification and redress (Articles 11-13)

3.1.10.1 Access (Article 11) – How an individual can see the data held about them
The June 2015 DHS Privacy Office Privacy Compliance Review Report on the use and transfer of passenger name records between the European Union and the United States states that DHS had not refused any passenger access to his or her PNR. The report detailed that DHS received 42,028 access requests for "travel records" during the reporting period. This represents an increase of almost 150% since the 2013 report. Out of all the requests received by DHS, 342 were specific requests for PNR and 24% of these (approximately 82) were EU-related. DHS informed that the average response time to requests of travellers is 180 days – this is reportedly due to the increase in the overall number of requests received across all subjects, not just PNR. This compares with 38 days as reported in the 2013 joint review. The DHS target response time is 25-30 days.

Conclusion: DHS has complied with Article 11 of the Agreement by not refusing any passenger access to their PNR. The increase in average response time is considerable since the last review and provides cause for concern. Consideration should be given to increasing the number of staff available to process requests for PNR in order to reach the target response time.

Recommendation:
***7)* DHS should lower the average response time for passenger access requests to PNR.**

3.1.10.2 Correction (Article 12) – How an individual can correct data held about him or her
No enquiries have been received for correction, rectification, erasure or the blocking of an individual's PNR.

Conclusion: Whilst this Article has not yet been tested, the processes detailed in Article 11 exist and appear compliant with the Agreement. As noted under 3.1.9, DHS should continue to ensure that the public are informed about their rights and are given contact details should they wish to correct the data held about them.

3.1.10.3 Redress (except for transparency on redress mechanisms) (Article 13) – How an individual can appeal to correct, rectify or delete information held about him or her
A representative of the US Department of Justice explained the then ongoing legislative process to extend judicial redress to non-US residents in the draft Judicial Redress Act. Since the joint review took place, the US Congress has enacted the Judicial Redress Act of 2015.

Between 1 June 2013 and 14 March 2015, DHS TRIP, which processes redress requests regarding travel related difficulties, received 31,509 enquiries[18] of which eleven enquiries were from individuals seeking redress for travel inconvenience that included references to a

[18] The Privacy Compliance Review - "Report on the use and transfer of passenger name records between the European Union and the United States", DHS Privacy Office, June 26, 2015 states on page 22 that between 1 June 2013 and 1 February 2015 the number of inquiries received by TRIP was 31,509.

traveller's PNR. While DHS TRIP does not require proof of citizenship or residency, based on text of the inquiries, one inquiry was EU related.

Conclusion: The enactment of the Judicial Redress Act is a welcome development and the EU PNR team will continue to follow progress.

3.1.11 Oversight (Article 14) – How compliance with the agreement can be monitored and subject to independent review

The DHS Privacy Office explained the nature of its work and the related checks and balances, which includes reporting to several committees of the Congress. The DHS Chief Privacy Officer may be addressed, if a complaint cannot be resolved by the CBP INFO Center or through DHS TRIP.

To provide further oversight and to ensure that DHS does not use PNR illegally or discriminate against individuals, the DHS Privacy Office is involved in the development and quarterly review of the targeting rules.

Conclusion: It is positive that the DHS Privacy Office has involvement in the development of targeting rules and can be approached by members of the public should a complaint not be resolved by the CBP INFO Center or through DHS TRIP. This is in accordance with Article 14 of the Agreement.

3.1.12 Method of PNR transmission (Article 15) – How the data should be transferred to the competent authorities covered by the agreement

DHS informed that it is important to keep the possibility to "pull" PNR, though it prefers that air carriers "push" data. The number of times DHS has pulled data has increased compared to the previous reporting period. However, it was not clear from the statistics provided whether the number of pulls of data collected under the Agreement (e.g. for flights with an EU nexus) had increased.

In response to the Commission's recommendation in the 2013 Joint Review Report, DHS has started to record the reasons why ad hoc "pulls" of data are used. DHS advised that the failure of airline systems was the main reason for using the "pull" method. DHS continues to support the PNRGOV standard for transferring PNR via the "push" method.

DHS confirmed that of the 54 air carriers covered by the Agreement at the time of our review, 50 have developed the capability to push PNR to DHS as required by the Agreement. DHS emphasised that the four remaining air carriers faced technical problems and did not oppose developing the ability to push data. After the review, the US confirmed that all carriers identified during the review are now providing PNR via "push". However, since the review, a new EU carrier which falls under the Agreement has started operating and does not have "push" capability. The US is working closely with the air carrier to develop "push" capability and cooperation has been positive.

Conclusion: The Commission will continue to follow this to ensure the US is receiving PNR "pushed" by carriers in line with the Agreement.

Recommendation:

8) DHS should continue to support and encourage all outstanding carriers to develop the capability to push PNR. To help manage this DHS should also improve statistical collection and reporting relating to the number of 'pulls' of data collected under the Agreement. The time periods for statistics must be consistent to enable direct comparisons to be made.

3.1.13 Domestic sharing (Article 16) – Sharing of data between US authorities

DHS confirmed that it shares PNR with other US authorities in accordance with Article 16 of the Agreement. Between June 2013 and April 2015, 2083 disclosures have been made to the National Counter Terrorism Center, 604 disclosures to the Federal Bureau of Investigation, 349 to the Drug Enforcement Agency, 140 to the Department of Defence, 72 to the US Postal Service, 59 to local law enforcement, 41 to the CIA and 21 to the Centers for Disease Control and Prevention. Disclosure forms are required for each external sharing of PNR.

Conclusion: Insufficient information was available to the EU team to conclude whether any of these cases would fall within the scope of the Agreement. There was also no opportunity to look in more detail at the disclosure form. Additional information, including an open text option on the disclosure form, would be beneficial to conclude whether any of these cases would fall within the scope of the Agreement. To ensure an assessment can be made, DHS should provide further details of why PNR was provided to other US authorities.

Recommendation:

9) DHS should provide further information regarding PNR data that has been shared with other US authorities. Statistical collection should increase to indicate how, why, when and by whom data is accessed by other authorities to support this recommendation. DHS should also provide information on exactly what data is collected under the Agreement. The time periods for statistics must be consistent to enable direct comparisons to be made.

3.1.14 Onward transfer (Article 17) – Sharing of data with third countries

DHS informed that no sharing of EU PNR with third countries (outside the EU) has taken place during the period of this review and there have been no emergency circumstances requiring the onward transfer of PNR.

Conclusion: This Article has not been tested, but mechanisms are in place to comply with this Article if required.

3.1.15 Cooperation with EU authorities (Article 18) – How the US works with Police, law enforcement and judicial bodies within the EU

DHS explained its cooperation with Europol through the CBP liaison officer at Europol, which indicates an increased sharing of PNR and of analytical information. However, DHS could confirm that CBP had been in direct cooperation on PNR only with the UK. Despite this, some Member States informed the Commission that they had received important information based on PNR from the US. Belgium has informed the Commission that in 2014 there were 11 cases in which US authorities provided analytical information without prompt. Furthermore in 2014 there were 16 cases regarding 28 individuals in which police or judicial authorities of Belgium requested PNR or relevant analytical information from the US. 100% of these requests were granted. One PNR for a citizen of Portugal was shared with the UK in compliance with article 18. DHS have since determined that between July 2014 and July 2015, DHS submitted 134 counterterrorism/terrorist travel reports to Europol that can be attributed to PNR data[19].

Conclusion: The US is in compliance with the Agreement and the Commission welcomes the ongoing cooperation with EU authorities. The US clearly does share information with the EU as demonstrated through the examples above; more details of how and when this takes place would be useful.

Recommendation:

10) DHS should record and provide further and improved information regarding how, why and when CBP shares PNR with Police, law enforcement and judicial bodies within the EU.

[19] Information provided in a letter from Chief Privacy Officer DHS to the Commission, dated August 12, 2015.

4. SUMMARY OF RECOMMENDATIONS

1) ***Article 2: Scope*** - DHS should record detailed reasons of why overrides have been used to better understand why they occur.

2) ***General:*** DHS should ensure that all facts and figures provided for subsequent reviews relate to the same time periods and solely to PNR which falls under the scope of this Agreement. This will provide a clearer basis for comparison.

3) ***Article 5: Safeguards*** - DHS should restrict the number of officers with access to PNR to those having a strict need to know.

4) ***Article 6: Sensitive data*** - DHS should regularly review the list of sensitive data codes and terms to ensure all sensitive information is being identified and automatically blocked by the system. Any changes to the list should be shared with the Commission.

5) ***Article 8: Retention of data*** - DHS should further investigate why a high number of PNR may have been inaccurately linked to law enforcement events and to take appropriate remedial action if necessary.

6) ***Article 8: Retention of data*** - DHS should regularly review the linking of PNR to law enforcement events to ensure PNR no longer required can be deleted as soon as possible.

7) ***Article 11: Access*** - DHS should seek to lower the average response time for passenger access requests to PNR.

8) ***Article 15: Transmission*** - DHS should continue to support and encourage all outstanding carriers to develop the capability to push PNR. To help manage this DHS should improve statistical collection and reporting relating to the number of 'pulls' of data collected under the Agreement. The time periods for statistics must be consistent to enable direct comparisons to be made.

9) ***Article 16: Domestic sharing*** - DHS should provide further information regarding PNR data that has been shared with other US authorities. Statistical collection should increase to indicate how, why, when and by whom data is accessed by other authorities to support this recommendation. DHS should also provide information on exactly what data is collected under the Agreement. The time periods for statistics must be consistent to enable direct comparisons to be made.

10) ***Article 18: EU Cooperation*** - DHS should record and provide further and improved information regarding how, why and when CBP shares PNR with Police, law enforcement and judicial bodies within the EU.

5. CONCLUSIONS

The EU team continues to find that the joint review mechanism is a valuable means of assessing DHS compliance with the Agreement. The joint review process has enabled the EU team to better understand how the data is used in practice and provided the opportunity for direct communication with targeting and analytical staff and other officials involved in the processing of PNR.

During the course of this joint review, **the EU team found that DHS implements the Agreement in accordance with its terms**. DHS continues to respect its obligations regarding the access rights of passengers and has an oversight mechanism in place to guard against unlawful discrimination. As previously noted, the US has transposed its commitments within this agreement into domestic rules through the publication of a System of Records Notice (SORN) in the U.S. Federal Register.

The EU team recognises the efforts made by the US to comply with this Agreement and the positive steps taken to implement all of recommendations from the 2013 review. However, DHS should continue to monitor its compliance with the Agreement and work to reduce its reliance on ad hoc pulls of PNR from a limited number of carrier systems.

It is noted that during the review 4 carriers were still not providing PNR via the "push" method. DHS has confirmed that from September 2015 all carriers identified at the time of the review were providing PNR via the "push" method.[20]

The number of staff with access to PNR has been raised by the EU team as a concern. Since the 2013 review, over 2000 more individuals have been granted access rights to PNR. Whilst the EU team is satisfied that oversight mechanisms are in place, it is important that the US monitors this issue and ensures that only those that have a pressing operational need to use and view the data can do so.

A number of recommendations are made to DHS in Chapter 3. These should be reviewed in the full evaluation of the Agreement due to take place in 2017.

[20] Whilst not included in the scope of this review, in September 2015 a new EU carrier which falls under the terms of this Agreement has started to operate but has not yet developed "push" capability. US DHS has confirmed that they are working closely with the carrier to develop "push" as soon as possible.

ANNEX A

EU QUESTIONNAIRE AND DHS REPLIES

Joint Review 2015 EU-U.S. PNR Agreement Questionnaire
Submitted by the European Commission May 5, 2015

SCOPE of Questionnaire: from the end of the last review in July 2013 to May 2015[21]

Questions of a general nature

Q1: *Have there been any unforeseen issues that have affected the implementation of this Agreement since the last review in 2013?*

Response: No. However, some operational and oversight responsibilities have shifted given the Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP), the DHS Privacy Office (PRIV), and the DHS Office of Policy (PLCY), as well as the DHS Traveler Redress Inquiry Program (DHS TRIP), have each undergone reorganizing and restructuring since the last review.

Q2: *Are all mechanisms required to properly implement the agreement, in particular those aimed at implementing the safeguards, in place and operating satisfactorily?*

Response: Yes.

Q3: *Have any specific incidents occurred since the last joint review in 2013 on the implementation of the agreement?*

Response: No.

Q4: *Do you have specific examples of PNR use or cases that prove the necessity of PNR in tackling terrorism and serious crime?*

Response: Yes. Specific examples of PNR use or cases that prove the necessity of PNR in tackling terrorism and serious crime will be shared with the delegation during the Joint Review.

I. General provisions

a) Article 2 – scope

Articles 2.2 and 2.3:

Q5: *Is the mechanism to filter out flights with no U.S. nexus still in place to ensure that the PNR data received regards solely flights with a U.S. nexus? Has this mechanism been audited and if so, which conclusions have been drawn?*

[21] July 10, 2013 – May 5, 2015 (unless otherwise noted).

Response: Yes, the mechanism to filter out flights with no U.S. nexus is still in place to ensure that PNR received by DHS regards solely to flights with a U.S. nexus. PNRs that are determined to be non-U.S. nexus are automatically blocked by the Automated Targeting System (ATS-P) and not stored in the database. The mechanism is audited by CBP management on an ad hoc basis to confirm the process is working properly. Additionally, information technology reviews also occur with random testing and analysis occurring on an ongoing basis. The results of these two processes confirm the mechanism to filter out flights with no U.S. nexus is performing as intended.

Q6: *Is the overriding functionality (operational since October 2009) still in place? If so, has it been audited since the audit in May 2013 and if so how many audits have taken place and which conclusions have been drawn?*

Response: Yes, the overriding functionality is still in place. As noted in the previous question, ATS-P is programmed to block those PNR it receives from airlines that do not contain U.S. airport codes. As explained more fully below, designated system users may initiate a manual override function to obtain PNR that has been inadvertently identified as non-U.S. nexus PNR. Use of the manual override function is audited and its use is tracked for compliance with CBP policy. When a user accesses what is or appears to be a non-U.S. nexus PNR, an email is sent in near real time for review to determine if there was a U.S.-nexus violation. The mailbox is reviewed routinely by a CBP Manager for mitigating action if warranted.

Q7: *How many times has the overriding functionality been used? For what purpose(s)?*

Response: There have been 1,571 override email notifications during the requested reporting period, from 290 different users. The purpose for these overrides is to alert the system that the traveler indeed does have a U.S. nexus, such as when an emergency landing or a known flight pattern includes a U.S. stop.

The increased number of overrides since the 2013 Privacy Compliance Review could be due to better accountability, a maturing oversight process, and improvements in RESMON. After management review, almost all of these overrides were ultimately found to have a U.S.-nexus. Since June 2013, there have been five warnings issued to CBP officers for accessing non-U.S. nexus PNR. These officers operated under the incorrect assumption that they were allowed to access these PNR. The appropriate CBP Manager followed up after the email notification was received, reviewed the PNR for a possible missed U.S.-nexus, told the officers they were not authorized to access non-U.S. nexus PNR, and reminded them of their obligations pursuant to the CBP PNR Directive.

Q8: *How is access to this functionality regulated?*

Response: When a user accesses what is believed to be a non-U.S. nexus PNR, an email is sent in near real time for review to determine if there was a U.S.-nexus violation. The mailbox is reviewed routinely by a CBP Manager for mitigating action if warranted.

Q9: *Is the override functionality still an exclusive pull mechanism? How does it relate to the agreed push method under Article 15?*

Response: Airline service providers have not provided an override push alternative that meets DHS/CBP's operational needs. As a result, all overrides continue to be via a pull of specific flight data.

b) Article 3 – provision of PNR

Q10: *Is the mechanism to filter out PNR data beyond those listed in the Annex to the Agreement still in place? Has this mechanism been audited and if so, which conclusions have been drawn?*

Response: Yes, the mechanism to filter out PNR beyond those elements listed in the Annex to the Agreement is still in place. During Privacy Compliance Reviews, CBP provided PRIV with PNR from randomly selected dates, which were analyzed to determine if any data elements beyond those listed in the Annex were present. PRIV found no data that CBP was not authorized to collect.

Q11: *Has DHS become aware of any additional type of PNR information that may be available and required for the purposes set out in Article 4 and if so, which?*

Response: No, DHS has not become aware of any additional type of PNR information that may be available and required for the purposes set out in Article 4.

Q12: *Has DHS become aware of any type of PNR information that is no longer required for the same purposes and if so, which?*

Response: No, DHS affirms that all 19 PNR data elements remain necessary for CBP's and the Department's mission.

Q13: *Has DHS ever used information held in PNR beyond those listed in the Annex, including sensitive information, and if so, how many times and for what reasons?*

Response: No, DHS has not used information held in PNR beyond those listed in the Annex.

c) Article 4 - the use of PNR data

Article 4.1:

Q14: *Is the PNR data shared under any other Programs? If so for which security purpose(s) is PNR being used under the Program(s) referred to? Have the Program(s) been audited and if so, which conclusions have been drawn?*

Response: PNR is only shared outside of DHS pursuant to Articles 16 through 18 of the 2011 Agreement and DHS's practices pursuant to those Articles are outlined later in this document.

PNR is used within DHS per the terms of Article 4 of the 2011 Agreement. Recently, in response to the current foreign fighter threat, DHS will temporarily copy[22] data from DHS databases certified to hold unclassified information to a DHS database certified to hold classified information. The privacy protections for this process are documented in a Privacy Impact Assessment (PIA)[23] for the DHS Data Framework – Interim Process to Address an Emergent Threat, which was provided to the European Commission on April 17, 2015.

As noted in answers provided in 2013, Immigration Advisory Program (IAP) and Regional Carrier Liaison Group (RCLG) CBP officers use PNR for authorized purposes and users with access to PNR are subject to the same use audits as any other PNR user.

Q15: *How do each of these Programs interrelate with each other?*

Response: PNR is used within DHS per the terms of Article 4 of the 2011 Agreement. The programs noted above do not "interrelate"; they are authorized users of PNR within DHS. The programs use PNR for the same purposes and under the same conditions as any other authorized DHS user. To that end, these programs use PNR is for the purpose of preventing, detecting, investigating, and prosecuting terrorist offenses and related serious transnational crimes.

Q16: *Has the override functionality already mentioned in the questions at a) for Article 2 of the Agreement been audited since May 2013 when the functionality was reviewed internally by DHS Privacy? Which conclusions have been drawn in particular as regards accessing PNR data from offloaded passengers that have not boarded an aircraft towards the US as they have been identified by DHS to be inadmissible prior to boarding through its Immigration Advisory Program (see also the question under Article 4.3)?*

Response: CBP Managers regularly review the appropriate use of the override mechanism and the Privacy Office reviewed the override functionality as part of the 2015 Privacy Compliance Review. IAP/CBP officers stationed in EU airports may receive PNR as part of their daily responsibility to determine if travelers with incomplete biographic data are a match to watchlisted individuals. In many instances, the IAP/CBP officers are able to obtain the missing traveler data from the air carrier and clear the traveler as a negative match without having to engage the passenger. If IAP determines that the traveler is likely to be inadmissible, the IAP officer will issue a no-board recommendation to the air carrier. PNR could assist the IAP/CBP officer in deciding to interview an individual or can be the basis for the officer's interview questions. The decision to recommend that the airline not board the passenger is, however, made based on the totality of the facts available to the officer.

<u>Article 4.2:</u>

Q17: *For how many case-by-case situations PNR data have been used?*

---

[22] This interim solution will only continue until the standard model is capable of meeting the mission. need. DHS remains committed to the standard model of the Data Framework for meeting DHS's mission need. DHS remains committed to the standard model of the Data Framework for meeting DHS's mission needs in the long-term, and the Department will revert to the standard model once the technical capabilities are available.

[23] http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhswide-dataframework-april2015.pdf.

Response: PNR data is an important component of CBP's evaluation of traveler data to identify high-risk travelers. CBP uses PNR data in conjunction with other data sets, including Advance Passenger Information (API), to process and evaluate travelers against watchlists and other potential risk indicators. Current intelligence and law enforcement information is also used to help define appropriate risk indicators. In addition to disclosures for terrorism related cases or active investigations of transnational crimes, CBP shared 21 PNR with the Centers for Disease Control and Prevention (CDC) during the review period to coordinate appropriate responses to health concerns associated with international air transportation, such as those surrounding the Ebola outbreak.

Article 4.3:

Q18: *How does this provision relate to the use of PNR data from passengers that have not boarded an aircraft towards the US as they have been identified by DHS to be inadmissible prior to boarding through its Immigration Advisory Program?*

Response: Article 4.3 notes that DHS uses PNR in order to identify passengers who may require further questioning or review, such as by an IAP/CBP officer prior to boarding. IAP officers make no further use of PNR data after a no board recommendation has been made.

Q19: *How many instances of denial of boarding have there been in response to PNR data?*

Response: Because PNR is but one component of CBP's evaluation of traveler data to identify high-risk travelers, we do not have an exact number of "no board" recommendations IAP/CBP officers have made to airlines based on PNR. Overall, IAP/CBP officers located at EU airports and Regional Carrier Liaison Groups officers have made 3,285 "no board" recommendations since July 2013 based on all sources of information available to them.

Q20: *Since the dates of the last review in 2013 how many individuals were targeted by ATS for further attention? How many of these were booked to travel on European flights?*

Response: DHS provided additional information to the EU Review Team in a confidential setting.

II. Safeguards applicable to the use of PNR

d) Article 5 - data security

Articles 5.1:

Q21: Which appropriate technical and organisational measures, in addition to the 2013 review, have been implemented to protect personal data and personal information contained in PNR?

Response: The CBP PNR Directive, updated in June 2013, remains in place to ensure the appropriate use, handling, and disclosure of PNR data that is maintained in ATS-P. The Directive provides a framework for granting access to PNR to authorized personnel within DHS and for sharing PNR data with DHS's domestic and international mission partners, as appropriate. Technical and organizational oversight is implemented by user access controls, biannual user access audits, log in and user warning banners, automated email alerts for

overrides or use of sensitive data, automated masking and depersonalization, and data retention limits.

Articles 5.2 and 5.6:

Q22: *Which encryption, authorisation, logging and documentation procedures are applied by DHS?*

Response: The CBP PNR Directive, updated in June 2013, remains in place to ensure the appropriate encryption, authorization, logging, and documentation procedures for PNR data that is maintained in ATS-P. Records in ATS are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies[24]. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. CBP has a number of physical and procedural safeguards to protect personal privacy and ensure data integrity, which include physical security, access controls, data separation and encryption, audit capabilities, and accountability measures. When information is transferred or removed from ATS, ATS logs the external sharing. Internal sharing is logged locally on hard copy, or the individual has an assigned account and ATS tracks the usage by the individual.

Q23: *Which measures are in place to ensure limited access to specifically authorised officials?*

Response: The CBP PNR Directive, updated in June 2013, remains in place to ensure limited access to specifically authorized officials of PNR data that is maintained in ATS-P. CBP uses access logs to verify that ATS-P users should be provided access to PNR and to determine if those users have a continued need or if their level of access is appropriate. Non-CBP users must be nominated by their Component manager with an appropriate justification for access, which is reviewed by CBP to determine if their need meets the purpose specification criteria for PNR access. Each user's level of access is also validated twice per year by supervisory and management review.

Q24: *How many specifically authorised officials have access to PNR data?*

Response: 14,414 DHS users have access to PNR in the "active" PNR database.

Q25: *In what secure physical environment is PNR being held and which physical intrusion controls are implemented to protect PNR? Has this environment changed since the previous review in 2013?*

Response: A system security plan for ATS was completed and an Authority to Operate (ATO) was granted to ATS for three years, on January 31, 2014. ATS processes, transmits, and stores personally identifiable information (PII). ATS has a FIPS 199 categorization of Confidentiality "MODERATE," Integrity "MODERATE" and Availability "MODERATE." Under FIPS 199, "MODERATE" is defined as "if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals." As a result, all records maintained in ATS, including

[24] At a minimum, DHS Sensitive Systems Policy Directive 4300A: https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf.

PNR, are stored electronically or on paper within secure facilities, in a locked drawer, and behind a locked door. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

Q26: *Which mechanism exists to ensure that PNR queries are conducted consistent with Article 4?*

Response: The mechanism that exists to ensure that PNR queries are conducted consistent with the PNR uses permitted under Article 4 of the 2011 Agreement is the CBP Directive regarding use and disclosure of PNR data. The 2013 Directive is available under the Help tab in ATS-P and outlines the appropriate use, handling, and disclosure of PNR data and provides a framework for granting access to PNR to authorized personnel within DHS and for sharing PNR with DHS's domestic and international mission partners, as appropriate. The 2013 Directive has been distributed throughout CBP and to other DHS PNR users with updated field guidance.
CBP has developed policy, in the form of this Directive, outlining the purposes for which PNR may be used. CBP also maintains a process of user access control, by which a user requiring access to PNR for his or her official duties must obtain prior supervisory approval before receiving access. Access to PNR is based on a user's job responsibilities and need-to-know, which align with the uses defined in Article 4. Each user's level of access is also validated twice per year by supervisory and management review. CBP's use of PNR in scenario-based targeting rules is also reviewed on a quarterly basis by DHS oversight offices, including the Privacy Office, the Office for Civil Rights and Civil Liberties, and the Office of the General Counsel.

Article 5.3:

Q27: *Which reasonable measures are taken to notify affected individuals in the event of a privacy incident? Have any such incidents occurred and if so, how many and what was their nature (unauthorised access, unauthorised disclosure, any other form of privacy incident)? Which remedial measures have been taken?*

Response: There were no privacy incidents involving PNR during the review period. If there were an incident, DHS adheres to Privacy Incident Handling Guidance[25], which establishes procedures delineating how to respond to the potential loss or compromise of PII.

Article 5.4:

Q28: *How many cases of significant privacy incidents were reported by DHS to EU authorities involving PNR of EU citizens or residents? Has any such incident occurred without such reporting?*

Response: There were no significant privacy incidents involving PNR of EU citizens or residents during the review period.

[25] http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf.

Q29: *What does DHS consider to be the relevant EU authorities?*

Response: If a significant privacy incident were to occur, DHS would begin engaging with the Embassies of the individuals affected by the breach in order to determine the European authority most capable of providing assistance to the affected individuals.

Article 5.5:

Q30: *What effective administrative, civil and criminal enforcement measures are implemented under US law for privacy incidents?*

Response: Disciplinary or corrective action regarding incidents caused by DHS personnel may be based on the following:

- Failure to implement and maintain security controls, of which an employee is responsible and aware, for PII regardless of whether such action results in the loss of control or unauthorized disclosure of PII;
- Exceeding authorized access to, or intentional disclosure to unauthorized persons of, PII;
- Failure to report any known or suspected loss of control or unauthorized disclosure of PII;
- For managers and supervisors, failure to adequately instruct, train, or supervise employees in their responsibilities; and
- For managers and supervisors, failure to take appropriate action pursuant to PII handling requirements upon discovering a Privacy Incident or failure to implement and maintain required security controls and to prevent a Privacy Incident from occurring.

Applicable consequences may include reprimand, suspension, removal, or other actions in accordance with applicable law and agency policy. At a minimum, DHS will remove the authority to access information or systems from any individual who demonstrates egregious disregard or a pattern of error in safeguarding PII.

Information technology security-related and privacy-related violations are addressed in the Standards of Ethical Conduct for Employees of the Executive Branch, 5 CFR Part 2635, and DHS employees may be subject to disciplinary action for failure to comply with DHS security and privacy policy, whether or not the failure results in criminal prosecution. Non-DHS federal employees or contractors who fail to comply with Department security and privacy policies are subject to termination of their access to DHS information technology systems and facilities, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions.

Penalties may also be imposed pursuant to the legal bases cited in DHS's response to the EU's 2013 questionnaire, including the Computer Fraud and Abuse Act (CFAA) (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2710 et seq. and 18 U.S.C. § 2510 et seq.), 18 U.S.C. § 641, and 19 C.F.R. § 103.34.

e) Article 6 – sensitive data

Article 6.1:

Q31: *Which automated systems does DHS employ to filter and mask out sensitive data from PNR?*

Response: Certain codes and terms that may appear in a PNR have been identified as "sensitive" and are blocked by ATS-P to prevent routine viewing.

Q32: *Is any sensitive data automatically deleted through the filter process rather than masked?*
DHS: CBP permanently overwrites the sensitive data after 30 days. The sensitive words and terms are permanently overwritten with no way to retrieve the sensitive information.

Article 6.2

Q33: *Has the list of sensitive codes already provided to the European Commission outlining what sensitive data will be filtered out been amended at all?*

Response: No, the list has not been amended. DHS continues to use the list of sensitive words and codes provided to the European Commission after the conclusion of the Agreement to filter terms in ATS-P.

Article 6.3:

Q34: *Since the last review in 2013 how many times have DHS staff accessed, used and/or processed sensitive data and for which type of circumstances?*

Response: CBP records indicate that no sensitive data has been accessed during the reporting period.

Q35: *In cases where sensitive data were used, how useful has it been in preventing the life of an individual to become 'imperilled or seriously impaired'?*

Response: CBP records indicate that no sensitive data has been accessed during the reporting period.

Q36: *Which restrictive processes are applied by DHS, and what are the experiences with the role of the DHS senior manager providing approval?*

Response: In exceptional cases where the life of an individual could be imperilled or seriously impaired, access to sensitive data may be granted upon approval of the Deputy Commissioner of CBP in consultation with the Assistant Commissioners (ACs) for the Office of Field Operations (OFO) and the Office of Intelligence (OI), DHS Office of Policy, and the DHS Chief Privacy Officer (the Chief Privacy Officer's approval may not be delegated below the level of Senior Director or component Privacy Officer), as appropriate. Any retrieval of sensitive PNR data through ATS-P will be recorded by the system. Sensitive information must be deleted within 30 days or upon conclusion of the action for which it was accessed, whichever is longer, unless retention of such data for a longer period of time is required by

law. Once an ATS user has been granted access to sensitive data and views a PNR containing such data, ATS will log the occurrence. A group of CBP managers receive a daily email indicating if a PNR with sensitive data has been accessed. CBP records indicate that no sensitive data has been accessed using this method during the reporting period.

Q37: *Has access to sensitive data without proper permission taken place? If so what were the consequences?*

Response: CBP records indicate that no sensitive data has been accessed during the reporting period.

Article 6.4:

Q38: *Regarding the 30 day retention period for sensitive data: What is considered the 'last receipt' of PNR data? What is the (approximate if necessary) time between the 'first receipt' of PNR data and the date of 'last receipt' of PNR data from which point the 30 day retention period begins?*

Response: DHS provided additional information to the EU Review Team in a confidential setting.

Q39: *Which measures have been taken by DHS to ensure that the data are permanently deleted after no more than 30 days from the last receipt of PNR containing such data?*

Response: When ATS-P ingests PNR, sensitive terms are automatically masked. There is no process to retrieve these sensitive terms after 30 days.

Q40: *In how many cases sensitive data have been retained for a time specified in US law for specific investigation, prosecution or enforcement actions?*

Response: There have been no cases of sensitive data being retained for specific investigation, prosecution, or enforcement actions.

f) Article 8 – retention of data

Articles 8.1 and 8.2:

Q41: *Which measures are in place to ensure the depersonalising and masking of the data sets listed under paragraph 2? Are these measures the same as detailed in the last review in 2013?*

Response: The automated processes within the ATS-P database to depersonalize and mask data have generally not changed since the last review in 2013, except that ATS-P is now programmed to automatically depersonalize PNR not connected to a law enforcement event six months, as recommended in the November 2013 European Commission report.

Q42: *After 6 months of the 5 year retention period in the active database the data is depersonalised and masked in line with the Agreement. Since the last review how many cases of re-personalisation of PNR records have there been?*

Response: The process to request to view depersonalized PNR and the process to determine who is authorized to access the depersonalized PNR continues to be updated based on mission and compliance needs. If authorized, the individual user is granted access to depersonalized PNR (however, this PNR remains depersonalized for everyone else). If an individual has a need for the repersonalized PNR, he must make a new request for the PNR to be repersonalized.

Q43: *What is the number of officials specifically authorised to access the active database?*

Response: 14,414 DHS users have access to PNR in the "active" PNR database.
Article 8.3:

Q44: *Do you have an update on the number of officials that will be / are specifically authorised to access the dormant database?*

Response: This is not confirmed yet due to the fact that PNR is not scheduled to move to the dormant database until 2017. Discussions to implement the dormant database are in its infancy.

Q45: *What form will the higher level of supervisory approval needed to access the dormant database take?*

Response: This is not confirmed yet due to the fact that PNR is not scheduled to move to the dormant database until 2017. Discussions to implement the dormant database are in its infancy.

Article 8.5:

Q46: *Has this paragraph been applied in practice yet? (Accepting that July 2017 is the date that data must start to be transferred to the dormant database have there been any exceptions?).*

Response: CBP will begin development in 2016 of the dormant PNR database, as the first PNR to be moved into dormant status will occur on July 1, 2017. PNR linked to a law enforcement event will be retained in the active database until law enforcement status is removed.

Q47: *What are the data retention requirements under US law that apply to this paragraph?*

Response: In accordance with the *Privacy Act of 1974*, each agency must publish notice of its systems of records (called a System of Records Notice (SORN)) in the Federal Register for all systems where information is retrieved from a group of records by some identifier of the individual under the control of any agency. As described in the Automated Targeting System (ATS) SORN,[26] the "retention period for the official records maintained in ATS will not

[26] http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm.

exceed fifteen years, after which time the records will be deleted, except as noted below. The retention period for PNR will be subject to the following further access restrictions: ATS users with PNR access will have access to PNR in an active database for up to five years, during which time the PNR will be depersonalized following the first six months retention. After this initial five-year retention, the PNR data will be transferred to a dormant database for a period of up to ten years. PNR data in dormant status will be subject to additional controls including the requirement of obtaining access approval from a senior DHS official designated by the Secretary of Homeland Security. Furthermore, PNR in the dormant database may only be repersonalized in connection with a law enforcement operation and only in response to an identifiable case, threat, or risk."

g) Article 9 – non-discrimination

Q48: *What measures are implemented to ensure that the safeguards to process and use PNR are applied to all passengers?*

Response: The 2013 CBP PNR Directive governs the processing and use of all PNR that CBP receives pursuant to its relevant statutory and regulatory requirements (49 USC § 44909 and 19 CFR 122.49d). Additional measures to ensure that the safeguards to process and use PNR are applied to all passengers are implemented by user access controls, biannual user access audits, log in and user warning banners, automated email alerts for overrides or use of sensitive data, automated masking and depersonalization, and data retention limits.

As required by the *Privacy Act of 1974* and the *e-Government Act of 2002,* DHS published the Automated Targeting System Privacy Impact Assessment and System of Records Notice to address mitigation of privacy risks associated with the Department's collection and use of PNR. ATS-P is programmed to apply automated safeguards to all PNR collected by DHS.

Q49: *In the last review in 2013 the implementation of a quarterly review process was raised. How have these quarterly reviews worked in practice in ensuring that PNR is not used to unlawfully discriminate against passengers?*

Response: The Privacy Office participates in quarterly reviews of ATS-P targeting rules with the Office for Civil Rights and Civil Liberties and the Office of the General Counsel, to ensure that the targeting rules are tailored to minimize the impact upon bona fide travelers' civil rights, civil liberties, and privacy, and are in compliance with relevant legal authorities, regulations, and DHS policies. The reviewing offices also review these rules to ensure that they are based on current intelligence identifying specific potential threats and are deactivated when no longer necessary to address those threats.

DHS addresses the use of ATS-P for targeting rules in annual data mining reports. The *Federal Agency Data Mining Reporting Act of 2007*, 42 U.S.C. § 2000ee-3, requires annual reports to Congress that provide an assessment of the impact or likely impact of the implementation of the data mining activity on the privacy and civil liberties of individuals, including a thorough description of the actions that are being taken or will be taken with regard to the property, privacy, or other rights or privileges of any individual or individuals as a result of the implementation of the data mining activity.

DHS exercises its authority[27] to engage in data mining in ATS-P, of which the DHS Chief Privacy Officer has reviewed for its potential impact on privacy. Decisions about individuals are not made solely on the basis of data mining results within ATS-P. In all cases, DHS employees conduct investigations to verify (or disprove) the results of data mining, and then bring their own judgment and experience to bear in making determinations about individuals initially identified through data mining activities.

h) Article 10 – transparency

Article 10.1:

Q50: *Has information to the travelling public been provided through the channels mentioned under (a) – (e)? Have any other appropriate measures as described under (e) been used? If so what are they?*

Response: Yes, DHS has provided information to the traveling public regarding its use and processing of PNR through publications in the Federal Register, on its websites, and through statutorily required reporting to Congress, including Privacy Office and Data Mining annual reports.

A PNR Frequently Asked Questions (FAQs) Document and a Privacy Policy Document are posted on the CBP website, and both were updated in June 2013 to reflect the 2011 Agreement.
The 2011 U.S.-EU PNR Agreement and previous reports of the DHS Privacy Office and joint reviews are posted on the DHS website at http://www.dhs.gov/privacy-foia-reports. For a comprehensive explanation of the manner in which DHS/CBP generally handles PNR data, the travelling public can refer to the Automated Targeting System (ATS) System of Records Notice (SORN)[28] and Privacy Impact Assessment (PIA)[29]. CBP's interim regulation regarding PNR is located in title 19, Code of Federal Regulations, section 122.49d, which is publicly available through multiple sources. In addition, CBP updated its "DHS/CBP Procedures for Access, Correction or Rectification, and Redress for Passenger Name Records (PNR)" with new contact information in June 2013. An earlier version of this document was available on DHS's website from July 2012 through the update.

Additionally, CBP has reached out to all affected air carriers individually or through industry associations via email and/or telephone to share appropriate notice language for carriers to incorporate into their contracts of carriage and to provide guidance that highlights changes implemented pursuant to the 2011 U.S.-EU PNR Agreement. Additional information on the DHS Traveler Redress Inquiry Program (DHS TRIP) process has also been shared with airlines and associations.

[27] Homeland Security Act of 2002, as amended.
[28] May 22, 2012 http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm.
[29] June 1, 2012 http://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_ats006b.pdf.

Article 10.2:

Q51: *Since the Review in 2013 has DHS updated its procedures and modalities regarding access, correction or rectification and redress procedures and has it provided the EU with such information for possible publication by the EU?*

Response: DHS continues to provide awareness of procedures regarding access, correction or rectification, and redress via the channels described above. There have been no updates since 2013 when this information was shared with the EU for its distributions and publication.

Article 10.3:

Q52: *What measures are implemented together with the aviation industry to encourage greater visibility to the public?*

Response: In addition to the information provided in response to the above question, the guidance provided to the affected air carriers also encouraged them to provide information to passengers at the time of booking regarding the purpose of the collection, processing, and use of PNR by DHS, and many carriers have posted information on their websites, some with links to the government sites provided.

i) Article 11 – access for individuals

Article 11.1:

Q53: *In the last Review DHS confirmed that the CBP tracking system deployed by DHS allows for the identification of requests for access to PNR data, including EU-originating PNR data. How many requests for PNR have been received from individuals? How many of these were EU related? What was the average response time by DHS?*

Response: CBP received 42,028 FOIA and Privacy Act requests since July 1, 2013, for "traveler data" of which 342 specifically requested PNR. The Privacy Office reviewed responses to all 342 PNR FOIA requests, and found that of those properly submitted, 24 percent were EU-related[30]. The average response time during the reporting period for all CBP FOIA requests is six months. (Note: the increase in processing time from 2013 is due to the increase in the overall number of FOIA requests CBP receives year after year, and the policy to process requests on a first in, first out basis.)

Article 11.2:

Q54: *In how many cases has disclosure of information been limited and for which reasons?*

Response: Under the terms of the System of Records Notice for ATS, which maintains PNR data, and the DHS Privacy Policy Guidance Memorandum 2008-01, CBP provides access to all persons requesting their own PNR. CBP has not limited disclosure of PNR to a requestor seeking access to her or his own PNR data.

[30] The DHS Privacy Office deems a FOIA request to be "EU related" if the requester claims citizenship, a mailing address, or place of birth in the EU.

Article 11.3:

Q55: *How many refusals or restrictions of access have been set forth in writing and provided to requesting individuals? What was the average response time by DHS?*

Response: CBP has not denied FOIA requests for PNR data. CBP, however, has notified requesters that their requests for PNR have been insufficient due to failures to provide required information including full name or date of birth, which is necessary to facilitate a proper search, or third party consent when applicable. The average response time for all CBP FOIA requests is six months.

Article 11.4:

Q56: *Has PNR data been disclosed to any other persons other than the requesting individual? If so how many times?*

Response: During this reporting period, there have been no FOIA responses to persons other than the requesting individual unless a third-party was authorized to seek the disclosure. Thirty-eight FOIA requests for PNR data were from an authorized third party. None of the authorized third-party FOIA requestors were identified as an EU Member State Data Protection Authority.

j) Article 12 – correction or rectification for individuals

Article 12.1:

Q57: *How many requests from individuals seeking for correction or rectification, erasure or blocking their PNR have been received by DHS?*

Response: DHS has received 11 inquiries that reference PNR from individuals seeking redress for travel inconveniences, but that do not specifically seek correction or rectification, erasure, or blocking of their PNR. During the reporting period, DHS had no cases from individuals who believed their personal data had been processed in a manner inconsistent with the Agreement, ATS PIA, or ATS SORN.

Article 12.2:

Q58: *In how many cases individuals were informed of DHS' decision to correct or rectify their PNR? What was the average response time by DHS?*

Response: Because DHS has not received any inquiries that seek correction or rectification, erasure, or blocking of an individual's PNR, there were no such notifications made.

Article 12.3:

Q59: *How many refusals or restrictions of correction or rectification have been set forth in writing and provided to requesting individuals? What was the average response time by DHS?*

Response: Because DHS has not received any inquiries that seek correction or rectification, erasure, or blocking of an individual's PNR, there were no refusals or restrictions made.

k) Article 13 – redress for individuals

Article 13.1:

Q60: *How many individuals sought administrative or judicial redress in accordance with US law (please make clear the distinction between those who are US citizens or legal residents and those who are not US citizens or legal residents and those that are EU related)? What was the outcome of this procedure?*

Response: Please note that because DHS TRIP does not request the citizenship of individuals seeking redress, our statistics are based on assumptions around information provided by the DHS TRIP filer in their inquiry.

Between July 3, 2013 and March 14, 2015, there were a total of 31,509 DHS TRIP inquiries[31] of which 7,062 applicants checked the Privacy box in their inquiry. During this period, DHS TRIP received 4,933 inquiries from individuals with an identified place of birth in the EU (compared to 5,729 inquiries from those with a place of birth in the U.S.) including 182 inquiries from individuals with an identified EU address (compared to 1,128 inquiries from those with a U.S. address) for a range of travel related concerns, not specifically PNR. The average time to process any type of inquiry is 54 days in Fiscal Year 2015.

Once an application and appropriate documentation is received by the Department and verified for completeness, DHS TRIP begins to process the request through the appropriate action office within DHS, the Department of State's Visa Office, and the Department of Justice's Terrorist Screening Center. CBP's TRIP office, which would receive all PNR related inquiries, has not received any DHS TRIP requests regarding modification or correction of PNR data, and therefore no DHS TRIP responses have been sent out regarding the issue. Additionally, CBP's TRIP office has not received any requests for judicial review or administrative challenges related to PNR. The length of the review varies based on the concerns raised by the redress requestor in his/her application. When the DHS TRIP review is complete, all relevant U.S. Government records are updated or corrected as appropriate. However, DHS TRIP cannot guarantee subsequent travel will be delay-free as additional screening or inspection may occur due to issues outside the redress process.

Article 13.2:

Q61: *In how many cases have individuals sought to administratively challenge a DHS decision related to the use or processing of PNR? What was the outcome of this procedure?*

Response: CBP's TRIP office, which would receive all PNR related inquiries, has not received any requests for administrative challenges related to the use of processing of PNR.

[31] Note that "inquiry" does not equal "person" as individuals can send in more than one application, sometimes for the same issue, sometimes for different ones.

Article 13.3:

Q62: *In how many cases has an individual decided to petition for judicial review in a US federal court of any final agency action by DHS? What was the outcome of this procedure?*

Response: CBP's TRIP office, which would receive all PNR related inquiries, has not received any requests for judicial review.

Article 13.4:

Q63: *Is the DHS Traveler Redress Inquiry Program (DHS TRIP) still the administrative means for individuals to resolve travel related queries?*

Response: Yes. DHS TRIP is the single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experience during their travel screening.

l) Article 14 – oversight

Article 14.1:

Q64: *How many complaints have been lodged with the DHS Chief Privacy Officer since the last review in 2013? What were the issues raised and what was the outcome of these complaints? What was the average response time by the DHS Privacy Office to such complaints?*

Response: There have been no complaints lodged with the DHS Chief Privacy Officer related to DHS collection or use of PNR since the last review in 2013.

Article 14.2:

Q65: *How many independent reviews were conducted by the DHS Office of Inspector General, the Government Accountability Office and the US Congress since the last review in 2013? If applicable, what were the outcomes of such reviews?*

Response: There have been no independent reviews conducted by the DHS Office of Inspector General, the Government Accountability Office, or Congress specific to DHS collection and use of PNR since the last review in 2013. During the 112th Congress, however, DHS use of PNR was addressed during a number of hearings and during general oversight hearings with former DHS Secretary Napolitano. Congressional officials have met with European Parliament delegations several times, both in the U.S. and in the EU, to discuss the issue.

Q66: *At the last review the EU team was informed of a new task to quarterly review the targeting rules used in relation to PNR. Have these reviews identified any cases where the PNR data was used unlawfully?*

Response: The Privacy Office reviews proposed targeting rules with the Office for Civil Rights and Civil Liberties and the Office of the General Counsel. These reviews have not identified any cases where PNR data was used unlawfully.

III. Modalities of transfer

m) Article 15 – method of PNR transmission

Article 15.4:

Q67: *All carriers should have acquired the technical ability to use the push method not later than 1 July 2014. What is the state of play?*

Response: On June 30, 2014, CBP confirmed that 16 of 16 covered carriers had acquired the technical ability to push PNR to DHS and were at various stages of implementation. For a carrier to change from a pull to a push transmission, there are many technical requirements. The transition from pull to push can be a lengthy process, with some of the connectivity aspects being handled by different entities within DHS. The technical nature of the transition from pull to push and the differences in the carriers' systems does not make for a completely standardized process and there can be additional complications to overcome (business changes for the carriers, funding for the project for the carriers, etc.).

As of May 18, 2015, out of the 54 carriers that are covered under the PNR Agreement, 50 have completed implementation and provide PNR via a push system.

Q68: *Does DHS still have access to PNR held by any air carriers via the 'pull' method?*

Response: DHS maintains a direct electronic connection to all but two covered carriers' reservation and/or departure control systems for the ability to pull data. This remains in place even for those carriers that are under a PNR push system in case there is a need for DHS to obtain a PNR on an ad hoc basis or for an override basis.

Q69: *How many carriers operating flights from the EU do not yet have a push system in place?*

Response: As of May 18, 2015, out of the 32 carriers that are covered under the PNR Agreement and operate flights from the EU, 28 completed implementation and provide PNR via a push system. The remaining four carriers are in the final stages of implementation of a push system. Dialogue between CBP and the four remaining carriers and/or their service providers is ongoing throughout this implementation process.

Article 15.5:

Q70: *In how many cases has DHS required carriers to provide PNR between or after the regular transfers described in paragraph 15.3 of the Agreement? Which method of transmission was used?*

Response: Since June 2013, there have been 3,541,944 circumstances when no PNRs were loaded from carriers, including from Push carriers and those carriers not yet pushing PNR. In some cases pulls occurred due to a flight schedule change, hardware or software issues on the carrier's end, or other connection issues. There were 531,823 additional pulls conducted by CBP field officers outside of the regular PNR transmission intervals where those officers needed an immediate refresh due to time sensitivities.

Q71: *Has DHS made a further assessment of its way of using the ad hoc functionality since completion of the internal review in July 2013 and if so, what were the findings?*

Response: Yes, DHS continues to assess how it uses the ad hoc functionality and how it meets operational needs. Since the July 2013 review, DHS has employed a mechanism for users to specify the reason for pulling a PNR outside of the normal automated process.

Q72: *Has DHS continued talks with the air carriers to find an acceptable ad hoc push functionality? If so, what is the state of play of such talks? If not, what are the reasons for not having pursued such talks?*

Response: As part of the PNRGOV International Standard, CBP has worked with the International Air Transport Association (IATA), air carriers, and service providers, along with other government representatives to include ad hoc push functionality as part of the standard. CBP continues to actively participate in PNRGOV meetings. As part of the PNRGOV message standard, there is an ad hoc push message that is called GOVREQ. The use of a GOVREQ must be mutually agreed upon between the government and the carrier to be implemented. DHS is not aware of any carriers actively pursuing GOVREQ and CBP has not agreed to use the GOVREQ message as an ad hoc push method and has no timeline in place to implement the use of GOVREQ. Because the pull method is already in place for ad hoc purposes with different connectivity than the push method, if a carrier or provider is having a connectivity or technical issue that is affecting their ability to push, CBP will still have the ability to access a PNR via the pull method. CBP continues to require that carriers maintain a pull connection for the times it is necessary for DHS to acquire a PNR on an ad hoc basis.

Q73: *How has DHS organised access to the ad hoc functionality? Has this approach changed since the last review? (Accepting the Agreement does not explicitly require limiting access to the ad hoc functionality to specifically authorised DHS officials).*

Response: Each user's access to the PNR ad hoc functionality is reviewed twice per year by the supervisor who authorized the role, and then validated by a CBP Headquarters Manager. This approach has not changed since the last review.

n) Article 16 – domestic sharing

Article 16.1.b:

Q74: *Which domestic government authorities has the DHS shared PNR data with? In what instances has this data been shared? In what volumes with each domestic authority has PNR data been shared?*

Response: Consistent with Article 4 of the Agreement, DHS will share information on high-risk travelers of interest who are under investigation for transnational crimes, terrorism, or when the sharing relates to health concerns. DHS will provide additional information on this sharing during the Joint Review.

Article 16.1.c:

Q75: *How does DHS guarantee that receiving authorities afford to PNR equivalent or comparable safeguards as set out in the agreement?*

Response: Receiving authorities will apply safeguards to the PNR pursuant to the CBP PNR Directive with affirmations in the PNR disclosure form and transfer letter. PNR disclosures are appropriately marked and include an attachment notifying the intended recipient that the PNR cannot be used for any purpose that is not consistent with the original purpose for their request. Additionally, the information cannot be released to any third party without the prior express written consent of CBP.

All EU PNR shared within the U.S. government includes the following caveat:
"This document is provided by the U.S. DEPARTMENT OF HOMELAND SECURITY (DHS)/U.S. CUSTOMS AND BORDER PROTECTION (CBP) to [insert authorized agency] for its official use only. This document contains confidential personal information of the data subject, including Passenger Name Record data ("Official Use Only"), which is governed by the Agreement Between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security. Such data must receive equivalent and comparable safeguards and be used only for the purposes outlined in the Agreement. This document may also contain confidential commercial information. The data is this document may only be used for authorized purposes and shall not be disclosed to any third party without the express prior written authorization of DHS/CBP."

o) Article 17 – onward transfer

Articles 17.1 and 17.2:

Q76: *According to paragraph 2, the US will fulfill the conditions of paragraph 1 by way of express understandings that incorporate data privacy protections comparable to those applied to PNR by DHS under the Agreement. How many such understandings have been entered into by the US?*

Response: The U.S. entered into understandings with Bulgaria and Europol during the reporting period. As both entities are legally bound to the terms of the U.S. – EU PNR Agreement, they should be legally bound to provide comparable privacy protections under EU law pursuant to 18.3(c), subject to the full scope of sanctions available to the European Commission should they fail to adhere to meet such a standard. To advance collaborative efforts to strengthen border security, combat transnational crime, and facilitate legitimate trade and travel, DHS entered into an agreement with Bulgaria for the Automated Targeting System – Global, an automated targeting tool to screen for passengers posing a potential risk. Additionally, CBP established a liaison officer at Europol to exchange law enforcement information with Europol partners, with a focus on disrupting terrorist travel.

Q77: *Have any 'emergency circumstances' occurred since the entry into force of the Agreement? If so, how many times and what type of emergency had to be faced?*

Response: CBP is not aware of any such emergency circumstances.

Article 17.3

Q78: *Where PNR data has been shared has this always been in compliance with article 17.3?*

Response: Yes, CBP is only aware of PNR being shared in compliance with article 17.3, only in support of those cases under examination or investigation.

Article 17.4:

Q79: *With which countries has PNR of EU Member State citizens or residents been shared? If applicable in what volumes has the data been shared with each of the countries?*

Response: A PNR for a citizen of Portugal was shared with the United Kingdom (which complies with Article 18).

Q80: *How many times has DHS informed an EU Member State that the US shared PNR of one of its citizens or residents with a third country? Did the Member State react to this sharing of information? Have there been situations in which a Member State was not informed and if so, why?*

Response: DHS has not shared EU PNR with any third countries during the reporting period.

p) Article 18 – law enforcement cooperation

Article 18.1:

Q81: *In how many cases did DHS provide analytical information obtained from PNR to relevant EU Member States authorities, Europol or Eurojust?*

Response: DHS has not shared "analytical information obtained from PNR" with relevant EU entities. However, under an existing written arrangement, DHS has shared one PNR with the United Kingdom Border Force for terrorism purposes and one PNR for transnational crime purposes. Additionally, there is a CBP Officer posted to Europol Headquarters as a liaison. The officer's role is to exchange law enforcement information with Europol partners, with a focus on disrupting terrorist travel. On a regular basis the liaison officer reviews reports on high risk passengers who were identified through advance targeting, including through PNR. When the liaison officer finds a targeted passenger with a nexus to a Europol member state, he shares the information in the report with the member state's representatives. Since October 2014, the DHS liaison submitted 122 names to Europol of persons suspected of being involved in terrorism.

The DHS Immigration and Customs Enforcement (ICE), Cyber Crimes, Child Exploitation Investigations Unit (CEIU) investigates U.S. citizens and/or lawful permanent residents who are arrested in, or traveled (are traveling) to, a foreign country and engage in illicit sexual conduct with minors. In support of this overall mission, the CEIU has developed Operation Angel Watch, a robust partnership with the CBP National Targeting Center – Passenger (NTC-P) to proactively identify and target Traveling Child Sex Offenders who are traveling to foreign countries. The NTC-P Advance Targeting Team (ATT) monitors the ATS-P Outbound Hot List for registered sex offenders with convictions for crimes against children. The ATT refers potential Traveling Child Sex Offenders targets to the CEIU for further analysis and dissemination to foreign law enforcement partners, via ICE Attaché offices, for action as they deem appropriate. From July 2013 to April 2015, DHS created 4,098 Angel Watch alerts resulting in 1,122 entry denials, including 528 referrals to EU Member States resulting in 21 entry denials.

Q82: *What criteria does DHS use to define 'as soon as practicable, relevant and appropriate' in order to provide analytical information obtained from PNR?*

Response: DHS views "as soon as practicable, relevant, and appropriate" to be directly tied to how the receiving EU Member State may utilize the data upon receipt. As such, a specialized decision based on the unique counterterrorism and law enforcement interests and capabilities of each Member State must be compared to the terms of the Agreement. DHS will not release information that cannot be operationally utilized consistent with the Agreement, including to EU Member States.

Article 18.2:

Q83: *How many requests did DHS receive from relevant EU Member States authorities, Europol or Eurojust for access to PNR or relevant analytical information obtained from PNR? If so, what was the nature of the specific investigation for which the data were requested, i.e. to combat terrorism and related crimes, or to combat transnational crime as described in Article 4?*

Response: DHS received two requests from the United Kingdom. The requests were for Transnational Crime and Terrorism.

Articles 18.3 and 18.4:

Q84: *How does DHS guarantee that the transfers respect the Agreement's safeguards and that equivalent or comparable safeguards are guaranteed by the receiving authorities?*

Response: Because the Agreement is binding on all Member States, they should be legally bound to provide such protections under EU law pursuant to 18.3(c), subject to the full scope of sanctions available to the European Commission should they fail to adhere to meet such a standard.

Nonetheless, DHS provides appropriate markings on any EU PNR data transferred under Article 18 under an existing authority to remind the recipient of this obligation. Such markings state:

> "This document is provided by the U.S. DEPARTMENT OF HOMELAND SECURITY (DHS)/U.S. CUSTOMS AND BORDER PROTECTION (CBP) to [insert authorized agency] for its official use only. This document contains confidential personal information of the data subject, including Passenger Name Record data ("Official Use Only"), which is governed by the Agreement Between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security. Such data must receive equivalent and comparable safeguards and be used only for the purposes outlined in the Agreement. This document may also contain confidential commercial information. The data in this document may only be used for authorized purposes and shall not be disclosed to any third party without the express prior written authorization of DHS/CBP."

ANNEX B

COMPOSITION OF THE REVIEW TEAMS

The members of the EU team were:

– Luigi Soreca, Security Director, European Commission, DG Home Affairs - Head of the EU Delegation

– Mattias Johansson, Policy Officer, Police Co-operation unit, DG Home Affairs, European Commission

– Horst Heberlein, Policy Officer, Data Protection unit, DG Justice and Consumers, European Commission

– Elise Latify, Legal Officer and Policy Officer, Commission nationale de l'informatique et des libertés (CNIL), France

– Simon Watkin, Senior Policy Advisor, Borders and Aviation Security Unit, Home Office, UK

– Elizabeth Roberts, First Secretary, Political, Development and Security Section, Delegation of the European Union to the United States of America, European External Action Service.

The members of the US team were:

– Karen L. Neuman, Chief Privacy Officer, Privacy Office, DHS

– Troy Miller, Executive Director, NTC, U.S. Customs and Border Protection

– Donald Conroy, Director, NTC-P, U.S. Customs and Border Protection

– Mario Medina, Director, NTC, Targeting Business Division, U.S. Customs and Border Protection

– Mike Cheatley, Program Manager, Office of Field Operations, U.S. Customs and Border Protection

– Shannon Ballard, Director, International Privacy Programs, Privacy Office

– Michael Borg, Branch Chief, Office of Field Operations, U.S. Customs and Border Protection

– Daniel Relay, Criminal Research Specialist, Homeland Security Investigations, Immigration & Customs Enforcement

– Michael Scardaville, Principal Director, Information Sharing, Threat Prevention and Security Policy, Office of Policy

– Clark Smith, Chief Information Officer, Office of Intelligence & Analysis

– David Hong, Office of the Chief Information Office, Office of Intelligence & Analysis

– Robert Neumann, Director, Traveler Entry Programs, U.S. Customs and Border Protection

- Jeannine Perniciaro, Program Manager, Traveler Entry Programs, U.S. Customs and Border Protection
- Kate Claffie, Acting Branch Chief, CBP Privacy Office, U.S. Customs and Border Protection
- Deborah Moore, Director, DHS Traveler Redress Inquiry Program
- Nael Samha, Director, Passenger Targeting, Office of Information Technology, U.S. Customs and Border Protection
- Thomas Burrows, Associate Director, Office of International Affairs U.S. Department of Justice