January 28, 2005

ENF-1-FO-NTS ETS

TO : Directors, Field Operations
Director, Preclearance Operations

FROM : Executive Director, National Targeting and Security /s/ Charles Bartoldus

SUBJECT: Requirements for Access to the Automated Targeting System - Passenger (ATS-P)

Passenger Name Record (PNR) data is some of the most sensitive data used by CBP to identify, target, and intercept persons intent on harming the U.S. Due to the sensitive nature of this data, and to protect personal privacies, CBP is taking a proactive approach in limiting access to sensitive passenger data to CBP employees with an official "need to know."

Authorized CBP employees can access risk-scored passenger information via CBP's computer systems via the Automated Targeting System – Passenger (ATS-P). Access to risk-scored passenger data is to be used strictly for enforcement purposes, including use in threat analysis to identify, interdict and exclude potential terrorists and other serious criminal offenders. Port and Field Office management are required to monitor access to passenger data to ensure only those CBP employees with a need to know have this access.

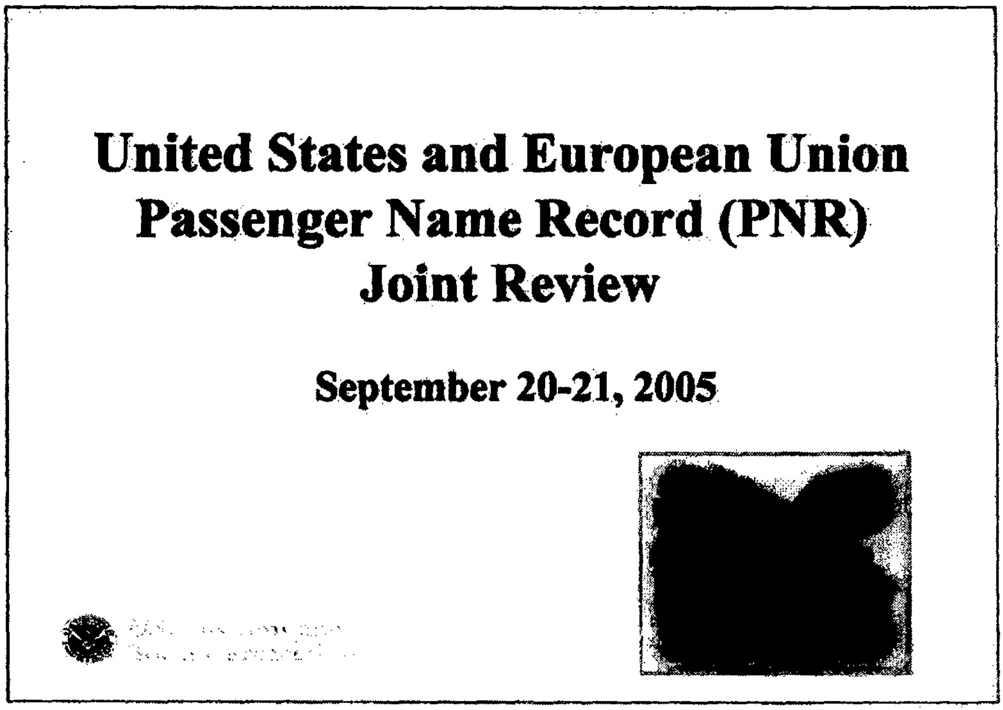
All new requests for access to ATS-P must be approved by the CBP employee's direct supervisor, (or other person designated by the employee's DFO), before being forwarded to the approving official at Headquarters, Office of Field Operations. The supervisor is responsible for determining if the requested access is necessary for the CBP Officer's performance of their duties. If approved by the supervisor, the request must be forwarded to (b6). of National Targeting and Security for final approval and processing. Only then can access to ATS-P be initiated.

If the CBP Officer no longer requires ATS-P access to perform their duties (e.g., change of work assignment or separation from CBP), then the supervisor is required to notify National Targeting and Security of this change. National Targeting and Security staff will remove access for any personnel who no longer require ATS-P and/or Resmon to perform their duties. The process for new requests for access to the Reservation Monitoring System (Resmon) were recently outlined in a memorandum dated December 30, 2004.

A recent review of officers with access to ATS-P and Resmon was conducted which identified a significant number of users who have not accessed these systems in the past 90 days. Due to the sensitive nature of the data and the requirement that only those personnel with a need to know can access the data, effective immediately, employees who have failed to log in to either ATS-P or Resmon within a 90-day period will lose access to that system. If an employee requests to be reinstated, the DFO is responsible for verifying and notifying National Targeting and Security of the employee's need to retain access to ATS-P and/or Resmon.

As a reminder, please ensure that all employees who are authorized access to PNR information have signed a receipt upon receiving these guidelines per the following memorandum "Field Guidance Regarding Use and Disclosure of Passenger Name Record Information (PNR) (ACTION: TC# BSF 05-0362: Due: Immediately)" dated December 20, 2004. Additionally, each employee's supervisor is responsible for recording their employee's receipt of the above document in(   ) using the course b2 high/b7E titled, **"FIELD GUIDELINES FOR USE OF EU PNR DATA,"** course code number **078005.**

If you have any questions, please have your staff contact (b6), at (b2, b6) or (b2)

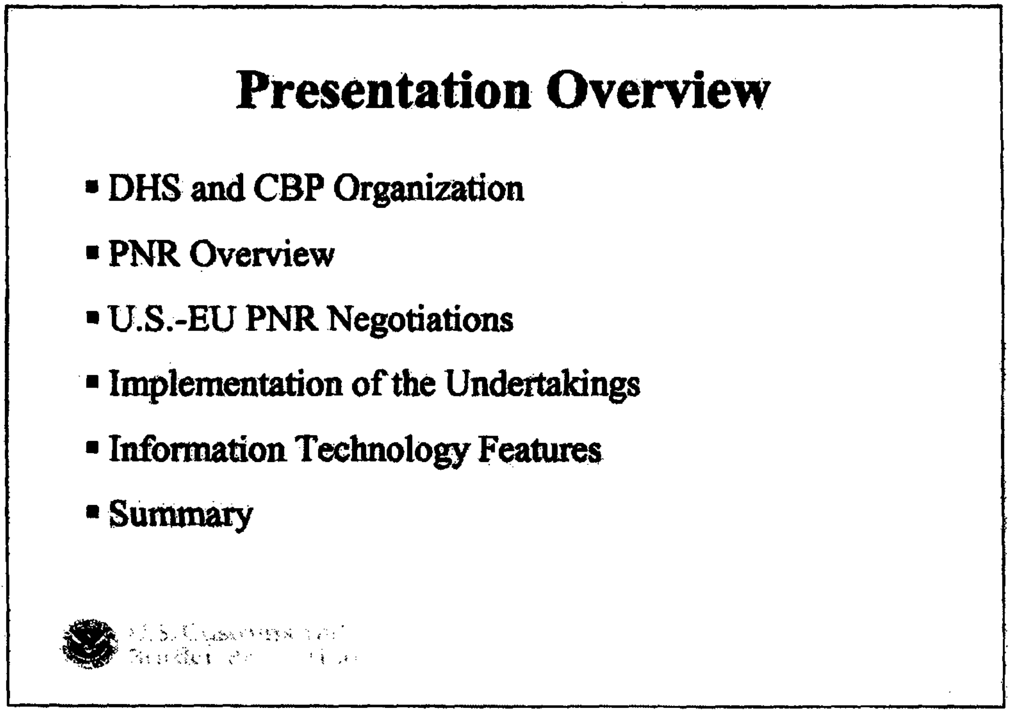


United States and European Union Passenger Name Record (PNR) Joint Review

September 20-21, 2005

Good Morning, thank you for being here and participating in the first Joint Review of the PNR agreement between the United States and the European Union. I am Robert Jacksta, Executive Director, Border Security and Facilitation.

As you may know my agency has been tasked with the priority mission of securing our nation's borders and protecting national security PNR information is an essential tool in these efforts.

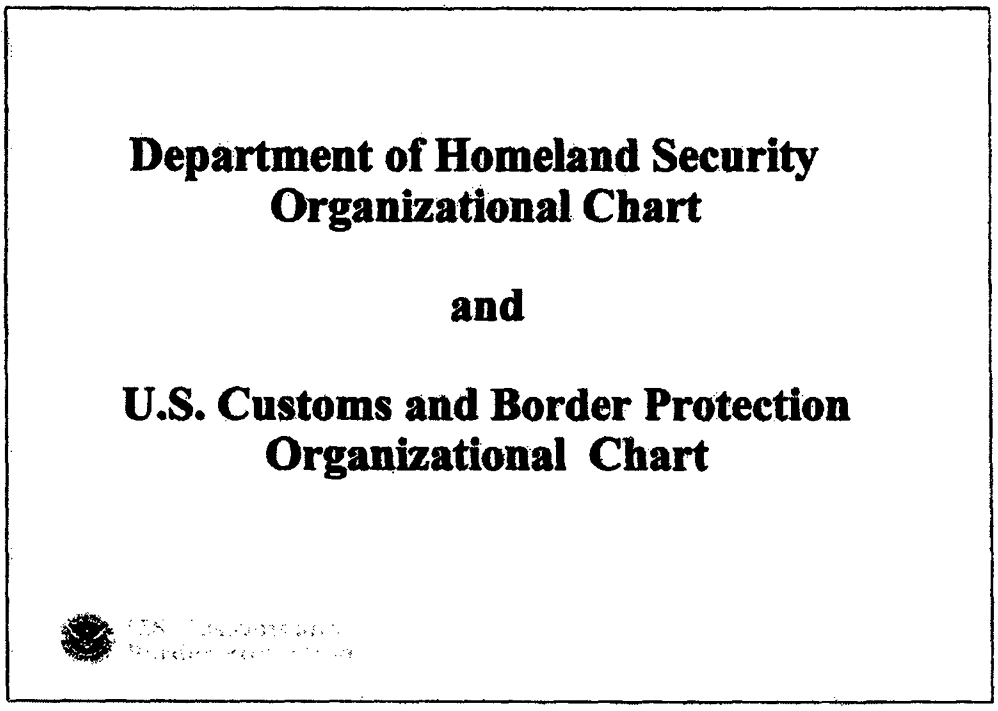


Presentation Overview

- DHS and CBP Organization
- PNR Overview
- U.S.-EU PNR Negotiations
- Implementation of the Undertakings
- Information Technology Features
- Summary

U.S. Customs and
Border Protection

Explain how the presentation will be focus on these main areas.

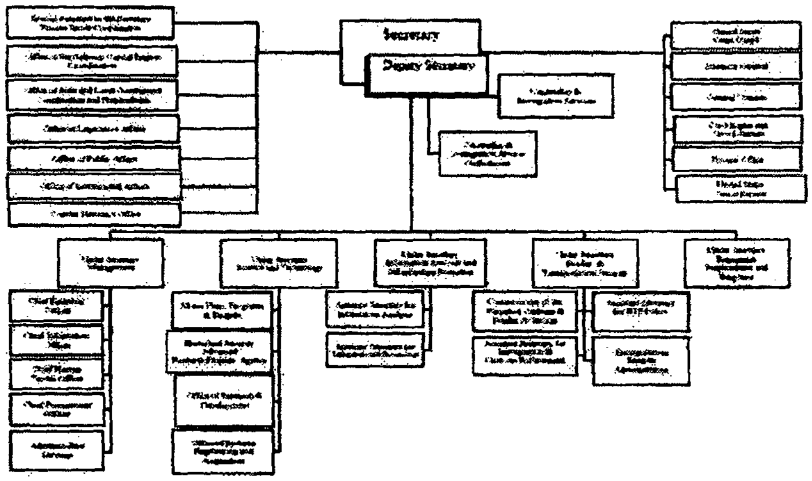


Department of Homeland Security Organizational Chart

and

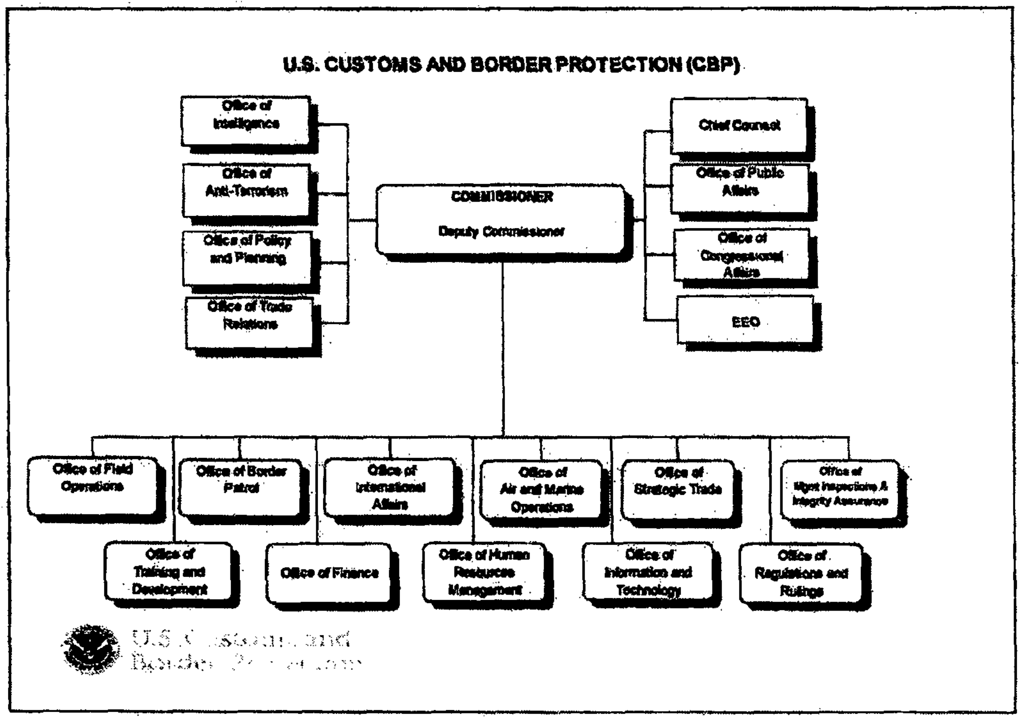
U.S. Customs and Border Protection Organizational Chart

Department of Homeland Security



U.S. Customs and
Border Protection

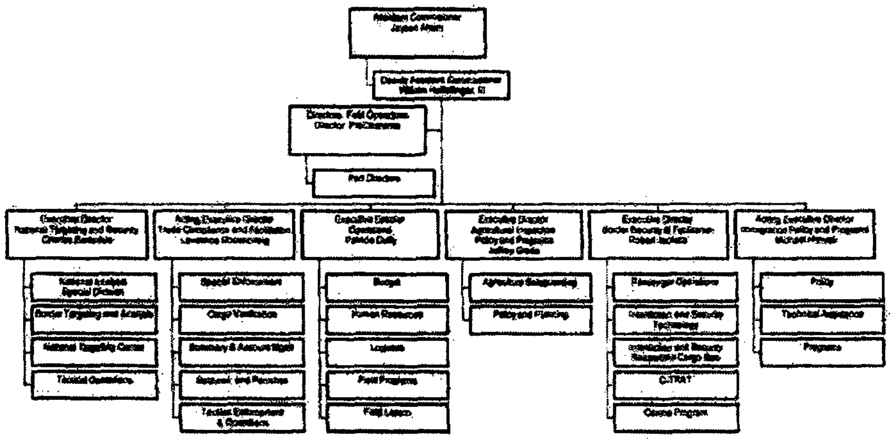
The Department of Homeland Security was accomplished to help increase communication, coordination, and resources within our emergency and border agencies. DHS has three primary missions: prevent terrorist attacks within the U.S., reduce America's vulnerability to terrorism, and minimize the damage from potential attacks and natural disasters. One of the top priorities was to integrate specific departmental functions to enhance efficiencies and create greater accountability in one seamless border service and that was accomplished on March 1, 2003.


U.S. CUSTOMS AND BORDER PROTECTION (CBP)
Office of Intelligence
Office of Anti-Terrorism
Office of Policy and Planning
Office of Trade Relations
COMMISSIONER
Deputy Commissioner
Chief Counsel
Office of Public Affairs
Office of Congressional Affairs
EEO
Office of Field Operations
Office of Border Patrol
Office of International Affairs
Office of Air and Marine Operations
Office of Strategic Trade
Office of Mgmt Inspections & Integrity Assurance
Office of Training and Development
Office of Finance
Office of Human Resources Management
Office of Information and Technology
Office of Regulations and Rulings
U.S. Customs and Border Protection

This is the organization chart for the components within U.S. Customs and Border Protection (CBP). CBP is the unified border agency within the Department of Homeland Security. CBP combined the inspectional workforces and broad border authorities of U.S. Customs, U.S. Immigration, Animal and Plant Health Inspection Service and the entire U.S. Border Patrol.

CBP includes more than 41,000 employees to manage, control, and protect the Nation's borders, at and between the official ports of entry. CBP has 317 official ports of entry and 14 preclearance offices in Canada and the Caribbean that is governed by the Office of Field Operations.

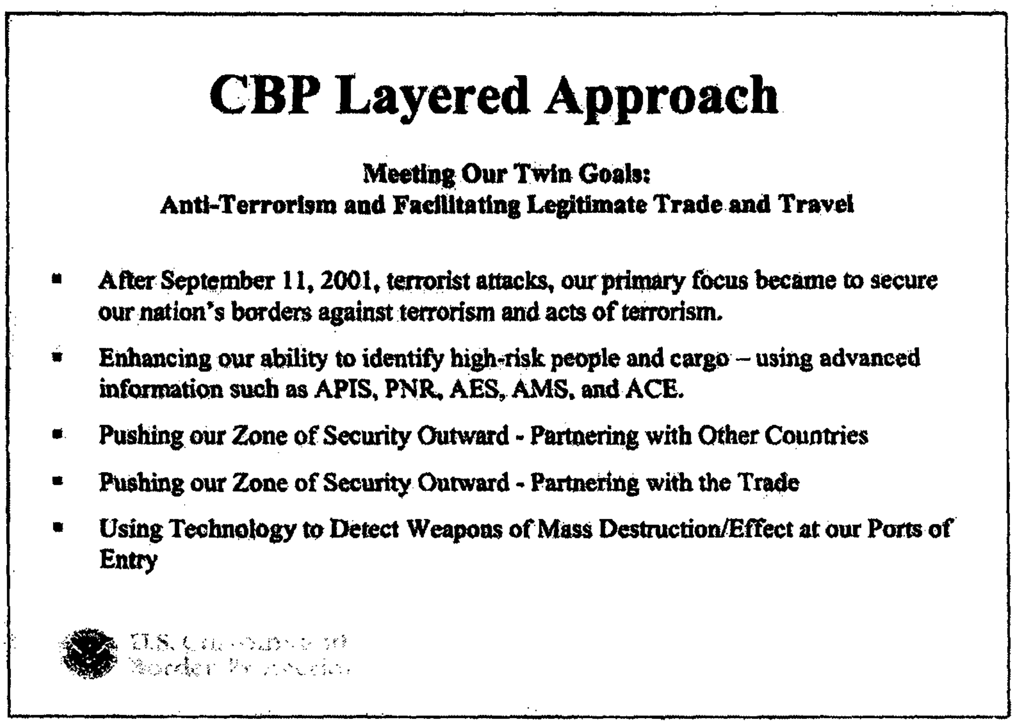
U.S. Customs and Border Protection
Office of Field Operations Organizational Chart


Assistant Commissioner Jayson Ahern
Deputy Assistant Commissioner William Heffelfinger, III
Director, Field Operations Director, Preclearance
Field Directors
Executive Director National Targeting and Security Charles Bartoldus
Acting Executive Director Trade Compliance and Facilitation Lawrence Thomas
Executive Director Operations Patricia Duffy
Executive Director Agricultural Inspection Policy and Programs Jeffrey Grode
Executive Director Border Security & Facilitation Robert Jacksta
Acting Executive Director Immigration Policy and Programs Michael Hrinyak
National Analysis Special Division
Border Targeting and Analysis
National Targeting Center
Tactical Operations
Special Enforcement
Cargo Verification
Summary & Account Mgmt
Seizures and Penalties
Tactical Enforcement & Operations
Budget
Human Resources
Logistics
Field Programs
Field Liaison
Agriculture Safeguarding
Policy and Planning
Passenger Operations
Interdiction and Security Technology
Interdiction and Security Passenger/Cargo Ops
C-TPAT
Canine Program
Policy
Technical Assistance
Programs

U.S. Customs and Border Protection

Office of Field Operations, (OFO) is the largest component of CBP. OFO has an operating budget of $2.2 billion and directs the activities of more than 25,000 employees, including more than 19,000 CBP Officers and Agriculture Specialists, and oversees the programs and operations at 20 Field Operations offices, 317 Ports of Entry and 14 Preclearance Stations in Canada and the Caribbean. OFO is comprised of the Immigration Policy and Programs that includes all immigration issues related to the admission and exclusion of aliens as well as the Agricultural Inspection at all Ports of Entry to protect the health of U.S. plant and animal resources and the facilitation of their movement in the global market place.

Additionally, OFO is responsible for Border Security and Facilitation, including Interdiction and Security, Passenger Operations, Targeting and Analysis and Canine Enforcement and for Trade Compliance and Facilitation which includes Cargo Entry and Release, Summary Operations, Trade Risk Management and Enforcement, and Seizures and Penalties as well as expanding Trade operations to focus on Anti-Terrorism.



CBP Layered Approach

Meeting Our Twin Goals:
Anti-Terrorism and Facilitating Legitimate Trade and Travel

- After September 11, 2001, terrorist attacks, our primary focus became to secure our nation's borders against terrorism and acts of terrorism.
- Enhancing our ability to identify high-risk people and cargo – using advanced information such as APIS, PNR, AES, AMS, and ACE.
- Pushing our Zone of Security Outward - Partnering with Other Countries
- Pushing our Zone of Security Outward - Partnering with the Trade
- Using Technology to Detect Weapons of Mass Destruction/Effect at our Ports of Entry

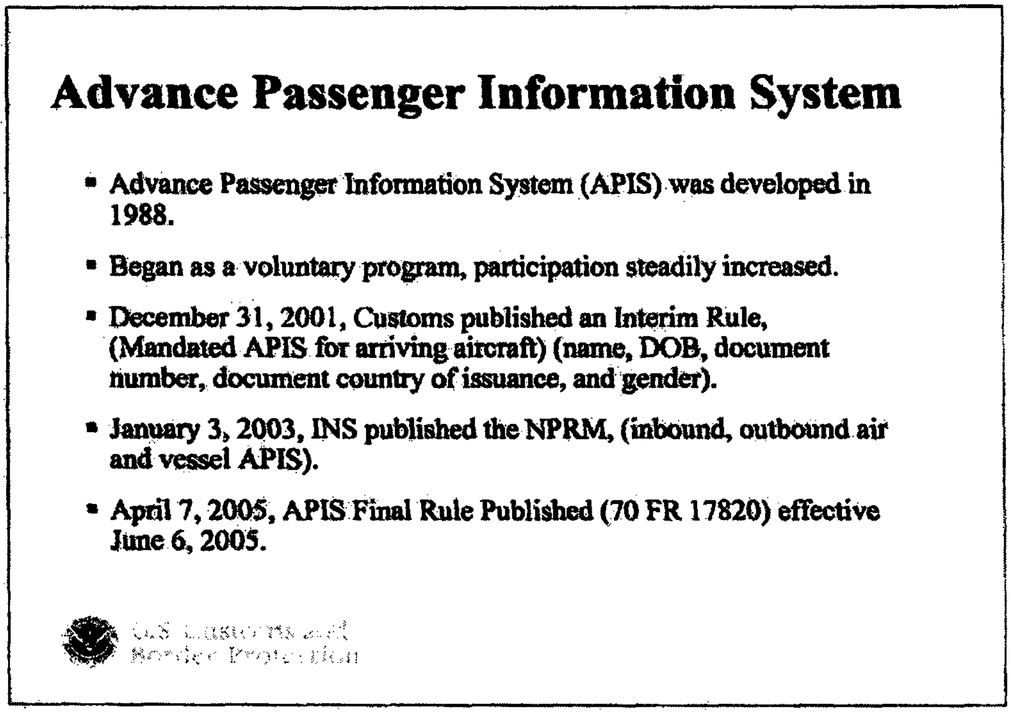
Meeting Our Twin Goals: Anti-Terrorism and Facilitating Legitimate Trade and Travel

- <u>Explain:</u> CBP's priority mission is preventing terrorist and terrorist weapons from entering the United States, while facilitating the flow of legitimate trade and travel.

- Advanced information enhances our ability to better identify people and/ or cargo that may pose a risk through these initiatives.
- Advance Passenger Information System (APIS), Passenger Name Record (PNR), Automated Export System (AES), Automated Manifest System (AMS), and the Automated Commercial Environment (ACE).

- Pushing our Zone of Security Outward - Partnering with the Trade – CTPAT, as well as acquiring PNR data from the airlines.

- Using Technology to Detect Weapons of Mass Destruction at our Ports of Entry – large scale Non-Intrusive Inspection equipment – x-ray and gamma ray machines, radiation portal monitors, and personal radiation detectors.



Advance Passenger Information System

- Advance Passenger Information System (APIS) was developed in 1988.
- Began as a voluntary program, participation steadily increased.
- December 31, 2001, Customs published an Interim Rule, (Mandated APIS for arriving aircraft) (name, DOB, document number, document country of issuance, and gender).
- January 3, 2003, INS published the NPRM, (inbound, outbound air and vessel APIS).
- April 7, 2005, APIS Final Rule Published (70 FR 17820) effective June 6, 2005.

U.S. Customs and Border Protection

<u>Explain:</u> APIS data elements received were:

Name, DOB, Document number, document country of issuance, and Gender.

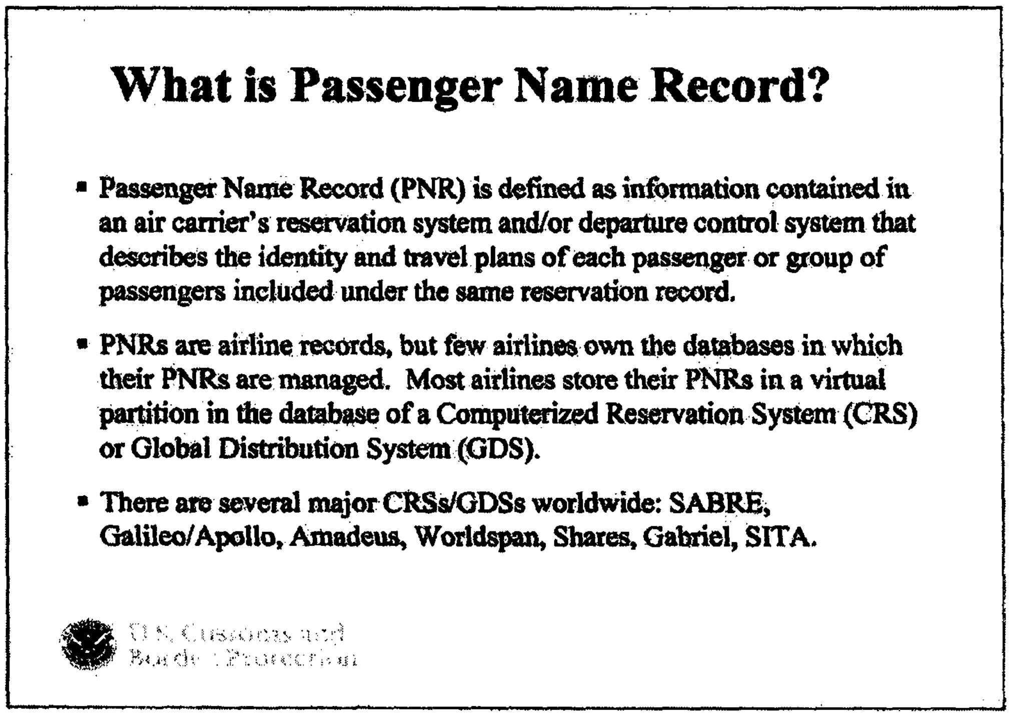
•Manifests run against law enforcement databases.Manifests queried against Automated Targeting Systems.

•Expedites processing of passengers through the FIS by reducing time to query each passenger.

• APIS allows CBP to focus enforcement on a few selected passengers while others quickly exit.

• APIS Final Rule expanded data elements, they are:

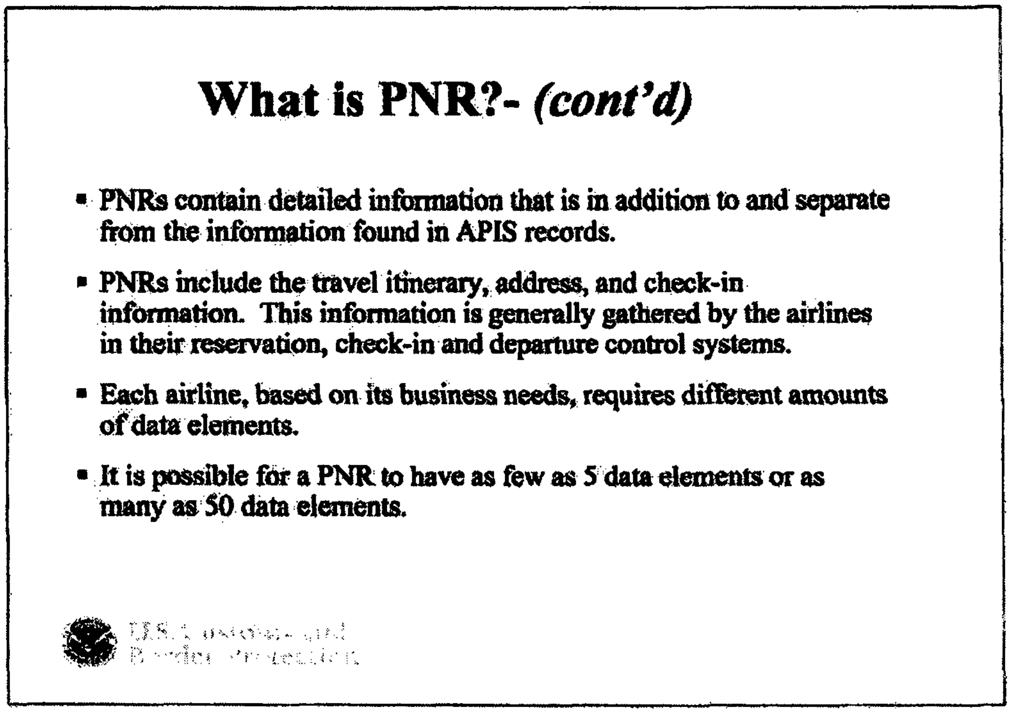
Citizenship, Country of Citizenship, Country of Residence, Status onboard the Aircraft, Travel document type, Passport expiration date, Alien Registration Number if applicable, Address while in the U.S., PNR Locator number.



What is Passenger Name Record?

- Passenger Name Record (PNR) is defined as information contained in an air carrier's reservation system and/or departure control system that describes the identity and travel plans of each passenger or group of passengers included under the same reservation record.
- PNRs are airline records, but few airlines own the databases in which their PNRs are managed. Most airlines store their PNRs in a virtual partition in the database of a Computerized Reservation System (CRS) or Global Distribution System (GDS).
- There are several major CRSs/GDSs worldwide: SABRE, Galileo/Apollo, Amadeus, Worldspan, Shares, Gabriel, SITA.

U.S. Customs and
Border Protection

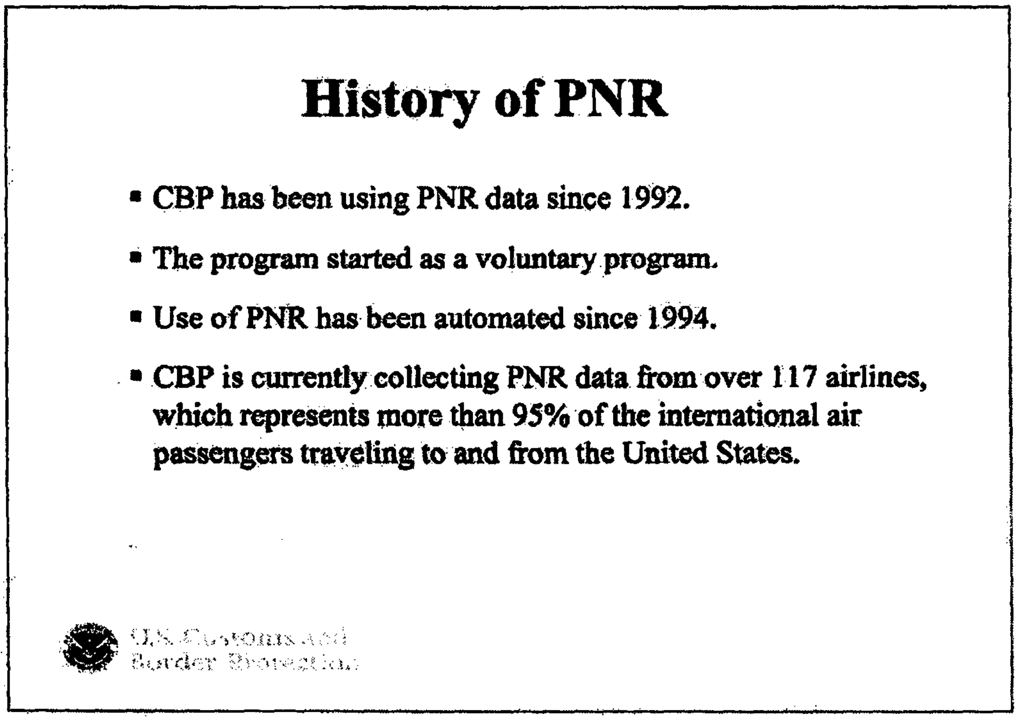


What is PNR?- *(cont'd)*

- PNRs contain detailed information that is in addition to and separate from the information found in APIS records.
- PNRs include the travel itinerary, address, and check-in information. This information is generally gathered by the airlines in their reservation, check-in and departure control systems.
- Each airline, based on its business needs, requires different amounts of data elements.
- It is possible for a PNR to have as few as 5 data elements or as many as 50 data elements.

U.S. Customs and Border Protection

A PNR may have many fields of information that have distinct components which may or may not be present in all PNRs.



History of PNR

- CBP has been using PNR data since 1992.
- The program started as a voluntary program.
- Use of PNR has been automated since 1994.
- CBP is currently collecting PNR data from over 117 airlines, which represents more than 95% of the international air passengers traveling to and from the United States.

U.S. Customs and Border Protection

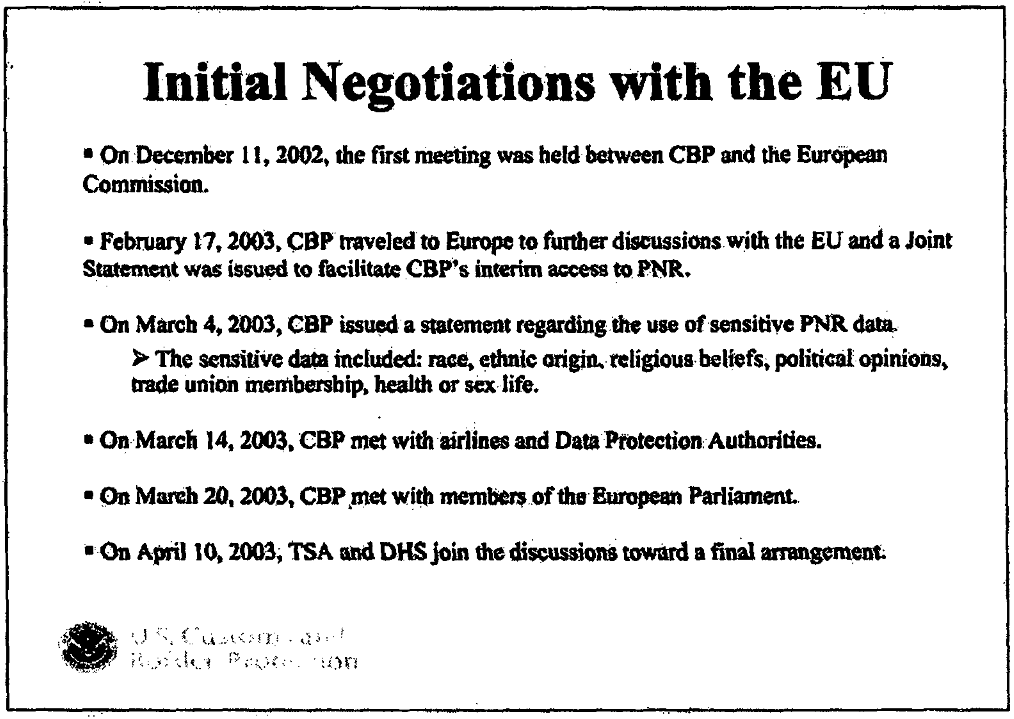
•The program started as a voluntary program. ?Before PNR became regulated, 14 airlines voluntarily electronically connected their reservation/departure control systems to CBP.

•American Airlines, Avianca, Aviateca, COPA, Continental Airlines, Delta Airlines, KLM, Lacsa, Nica, Northwest Airlines, Pakistan, TACA, US Airways, United Airlines

•Use of PNR has been automated since 1994. Started at 3 U.S. ports: Miami, Houston, and Dallas. Then expanded to other ports in 1997.

U.S.-EU PNR NEGOTIATIONS

U.S. Customs and
Border Protection



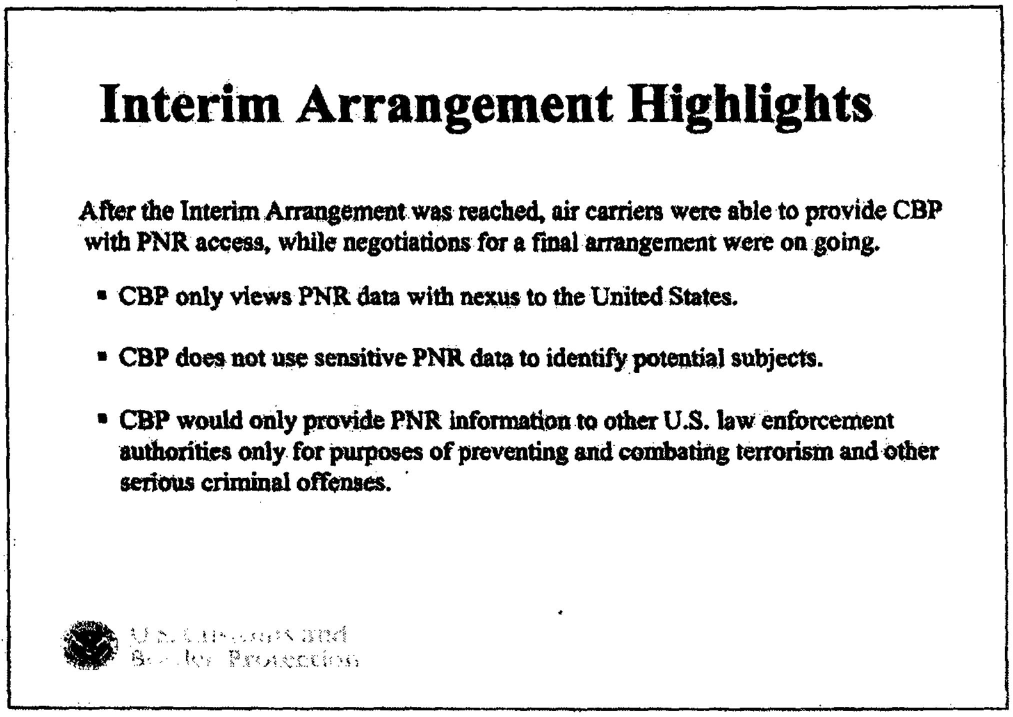
Initial Negotiations with the EU

- On December 11, 2002, the first meeting was held between CBP and the European Commission.
- February 17, 2003, CBP traveled to Europe to further discussions with the EU and a Joint Statement was issued to facilitate CBP's interim access to PNR.
- On March 4, 2003, CBP issued a statement regarding the use of sensitive PNR data.
  - ➢ The sensitive data included: race, ethnic origin, religious beliefs, political opinions, trade union membership, health or sex life.
- On March 14, 2003, CBP met with airlines and Data Protection Authorities.
- On March 20, 2003, CBP met with members of the European Parliament.
- On April 10, 2003, TSA and DHS join the discussions toward a final arrangement.

U.S. Customs and
Border Protection

▪Negotiations between the United States and the European Union was a lengthy, but productive process.

▪Concerns that the European Unions' (EU) data privacy directive (Article 25(6) of Directive 95/46/EC (the Directive) conflicts with CBP's Interim Rule were discussed.

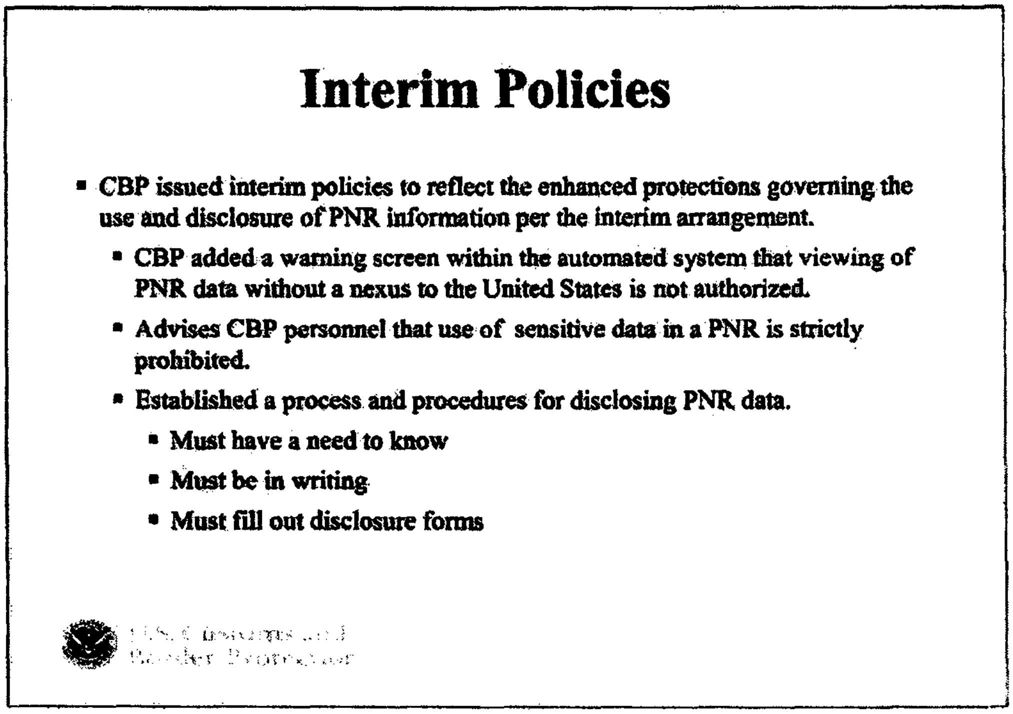


Interim Arrangement Highlights

After the Interim Arrangement was reached, air carriers were able to provide CBP with PNR access, while negotiations for a final arrangement were on going.

- CBP only views PNR data with nexus to the United States.
- CBP does not use sensitive PNR data to identify potential subjects.
- CBP would only provide PNR information to other U.S. law enforcement authorities only for purposes of preventing and combating terrorism and other serious criminal offenses.

U.S. Customs and Border Protection



Interim Policies

- CBP issued interim policies to reflect the enhanced protections governing the use and disclosure of PNR information per the interim arrangement.
  - CBP added a warning screen within the automated system that viewing of PNR data without a nexus to the United States is not authorized.
  - Advises CBP personnel that use of sensitive data in a PNR is strictly prohibited.
  - Established a process and procedures for disclosing PNR data.
    - Must have a need to know
    - Must be in writing
    - Must fill out disclosure forms

U.S. Customs and Border Protection

On July 22, 2003, CBP provided interim policies.

Explain: Advises CBP personnel that use of "sensitive data" in a PNR is strictly prohibited. The sensitive data elements include, but are not limited to race, ethnic origin, religious beliefs, political opinions, trade union membership, health or sex.

Explain: CBP has established policies and penalties (Table of Offenses and Penalties) in place that prohibits the use of this information in any of CBP's official duties.

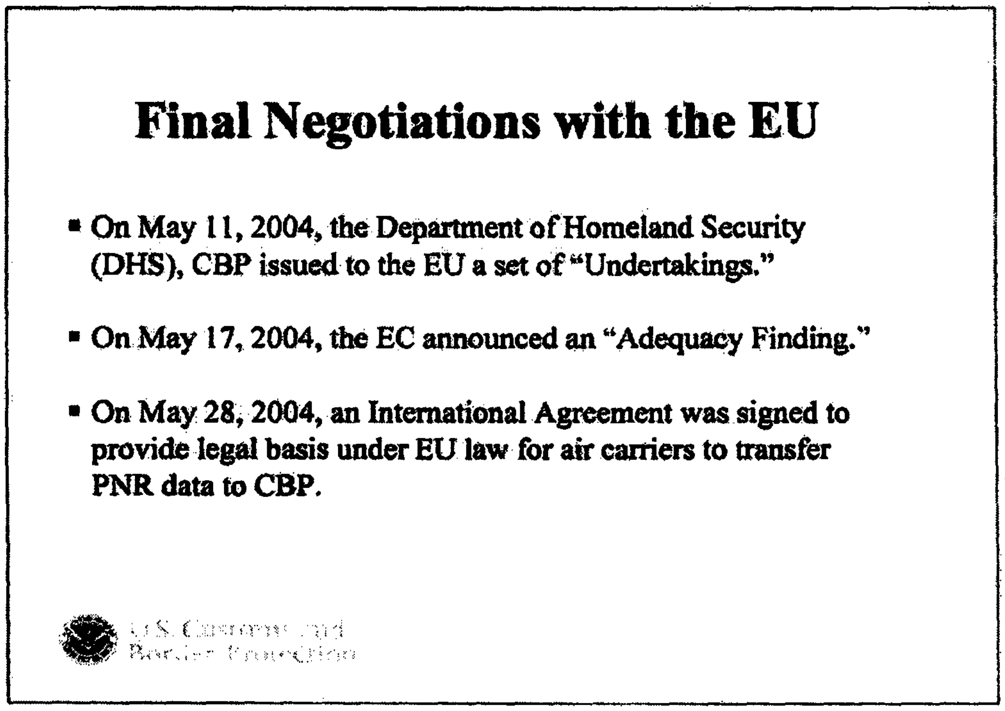
The interim guidance provide strict guidelines for the process and procedures for disclosing PNR data.

•Must have a need to know basis

•Must be in writing

•Must have supervisory approval

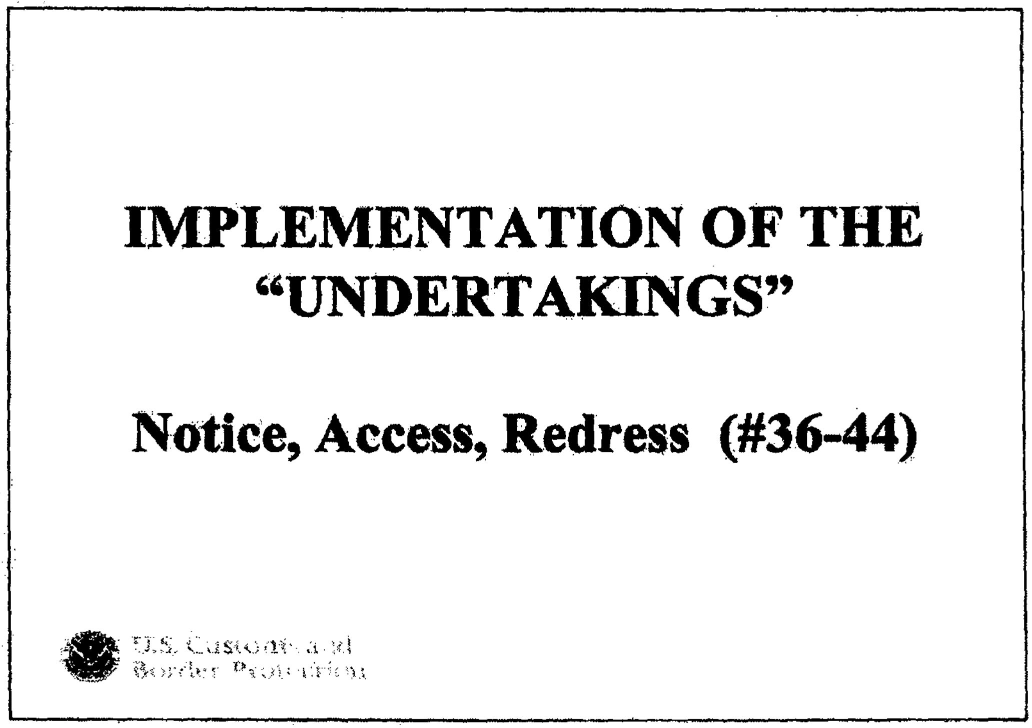
•Must fill out disclosure forms



Final Negotiations with the EU

- On May 11, 2004, the Department of Homeland Security (DHS), CBP issued to the EU a set of "Undertakings."
- On May 17, 2004, the EC announced an "Adequacy Finding."
- On May 28, 2004, an International Agreement was signed to provide legal basis under EU law for air carriers to transfer PNR data to CBP.

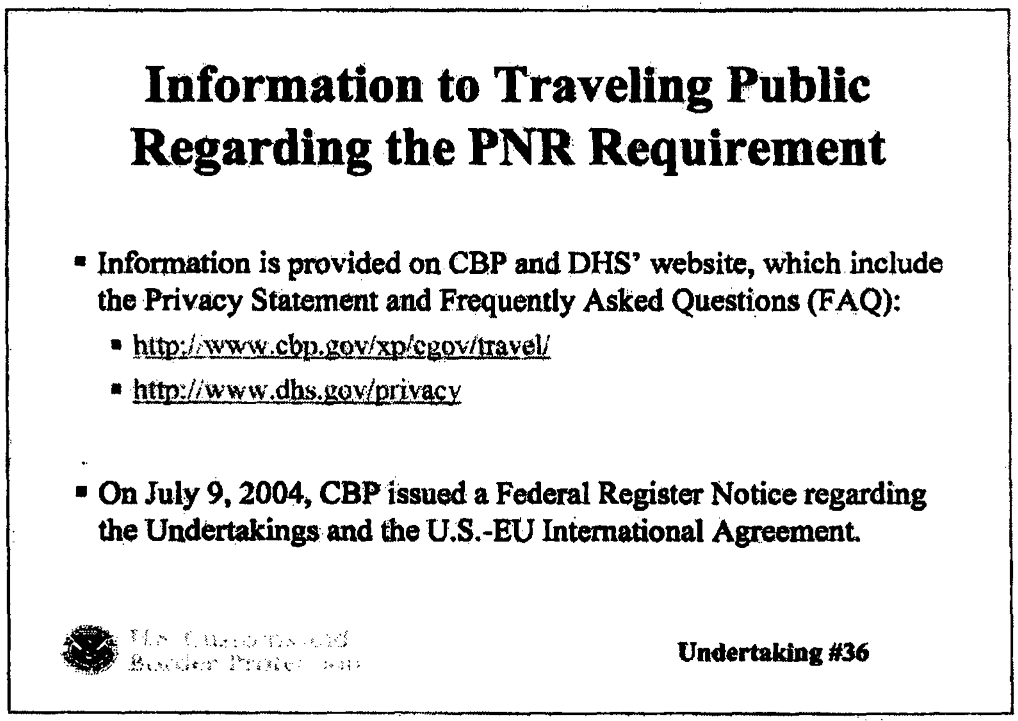
U.S. Customs and Border Protection



IMPLEMENTATION OF THE "UNDERTAKINGS"

Notice, Access, Redress (#36-44)

U.S. Customs and
Border Protection



Information to Traveling Public Regarding the PNR Requirement

- Information is provided on CBP and DHS' website, which include the Privacy Statement and Frequently Asked Questions (FAQ):
  - http://www.cbp.gov/xp/cgov/travel/
  - http://www.dhs.gov/privacy
- On July 9, 2004, CBP issued a Federal Register Notice regarding the Undertakings and the U.S.-EU International Agreement.

U.S. Customs and Border Protection

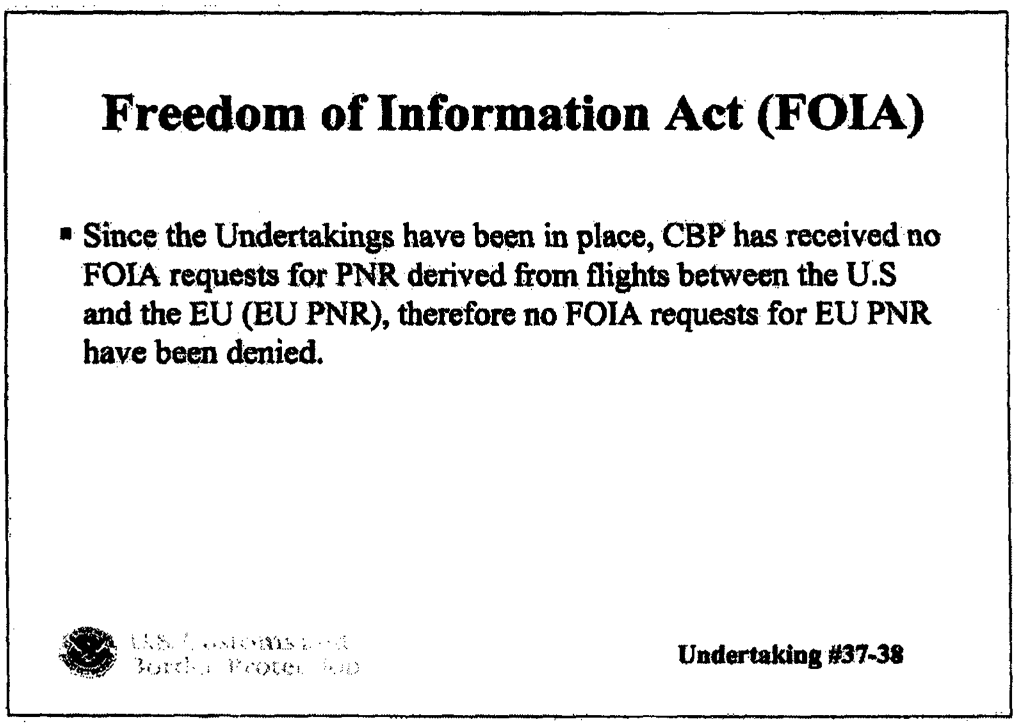
Undertaking #36

•CBP has added a privacy statement to DHS' website that can be linked from the CBP's website. It also include the Frequently Asked Questions.

Questions:

36) Please provide copies of passenger information such as travel pamphlets.

Included in this package is a copy of the notices. These can also be found on the CBP and DHS websites.



Freedom of Information Act (FOIA)

- Since the Undertakings have been in place, CBP has received no FOIA requests for PNR derived from flights between the U.S and the EU (EU PNR), therefore no FOIA requests for EU PNR have been denied.

U.S. Customs and Border Protection

Undertaking #37-38

•Before the Undertakings were in place, two FOIA requests were received by the Privacy Office.
No PNR data was available for data subject.

•DHS Privacy Office has received two FOIA requests (one data subject from Belgium, the other data subject from Spain) seeking copies of EU PNR information, both were prior to the issuance of the Undertakings.

•CBP has not denied or postponed disclosures of PNR record to any first party requestor.

Questions:

37) Have any requests been made by data subjects to receive a copy of PNR data contained in CBP databases? If so, how many requests have been made by data subjects, and from which countries?

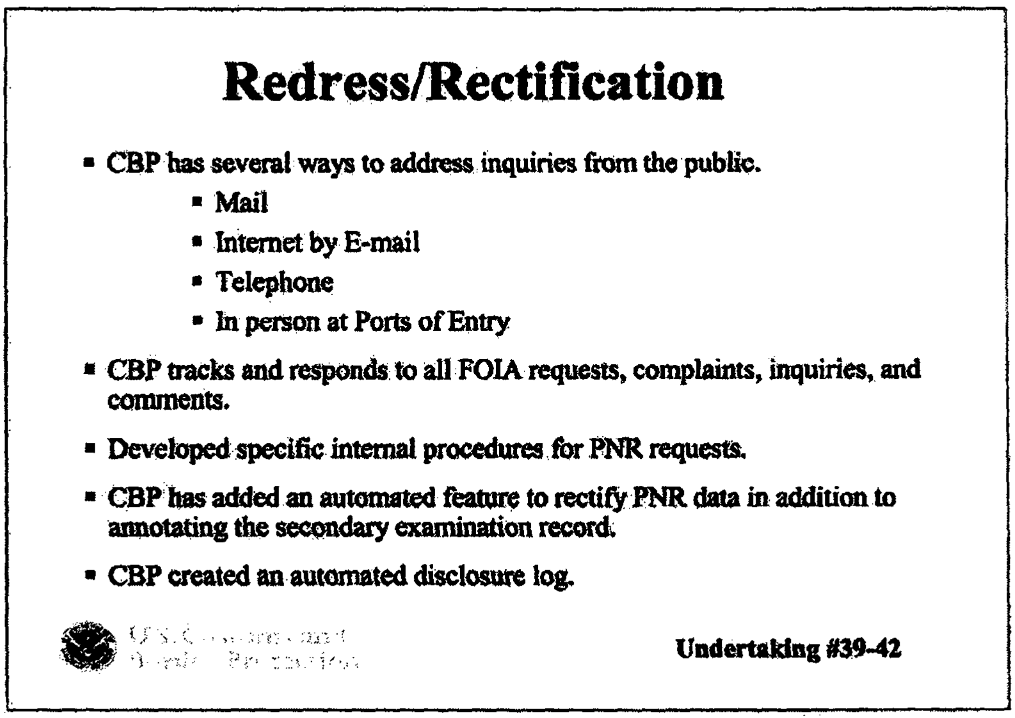
Since issuance of the Undertakings, CBP has received no FOIA requests seeking a copy of EU PNR data contained in CBP's databases, as contemplated by this paragraph of the Undertakings. As noted above, two FOIA requests seeking copies of passenger information (both prior to the issuance of the Undertakings) were received by the Privacy Office; the requesters were a data subject from Belgium, and a subject from Spain through the Spanish Protection Authority.

38) Have there been denied or postponed disclosures of the PNR record to a first party requester?

No, none to date.

If so, how many? In whole or in part relating to PNR? In which cases have disclosures been denied or postponed in whole or in part relating to PNR? *N/A*

Have there been any judicial challenges? *N/A*



Redress/Rectification

- CBP has several ways to address inquiries from the public.
    - Mail
    - Internet by E-mail
    - Telephone
    - In person at Ports of Entry
- CBP tracks and responds to all FOIA requests, complaints, inquiries, and comments.
- Developed specific internal procedures for PNR requests.
- CBP has added an automated feature to rectify PNR data in addition to annotating the secondary examination record.
- CBP created an automated disclosure log.

Undertaking #39-42

•FOIA and Privacy Act requests are handled by CBP through existing CBP procedures by way of mail, internet by e-mail, by telephone or they may hand deliver comment cards or make complaints to supervisors at the ports of entry.

•CBP has a dedicated unit that address all FOIAs and a separate unit that address inquiries and complaints. All FOIA requests, comments, complaints and responses are tracked.

•CBP has also developed procedures to specifically address FIOA requests pertaining to PNR issues and tracks them separately.

•Once a request is received from a data subject, if the information in a PNR is determined to be inaccurate, CBP will annotate the passenger's secondary examination record to reflect the inaccurate information.

• CBP has added an automated feature that would allow a note of the correct information to be linked to the appropriate PNR.

•CBP has established an automated disclosure log to better identify any Designated Authorities which have received such PNR data and notify them of any material that has been rectified.

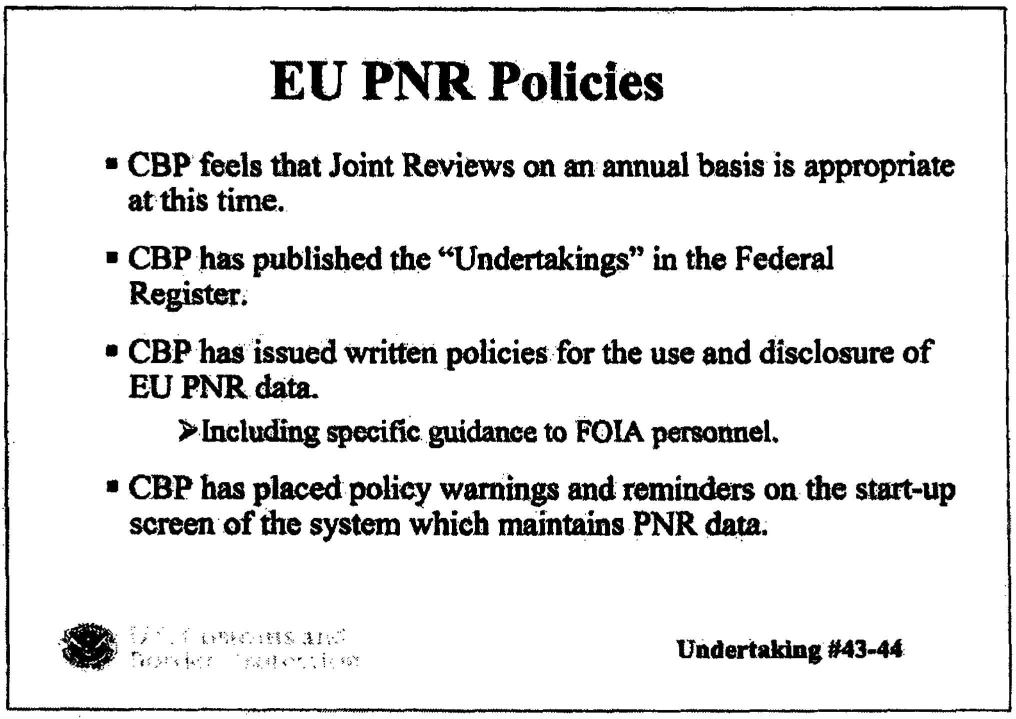
•To date, CBP has received no complaints or requests for rectification

Questions:
39) Have any requests been made to rectify data?
No, none to date.
If so,
(a) How many such requests have been made by passengers and crew members, air carriers or data protection authorities (DPAs) in the EU? Which data were concerned? *N/A*
(b) In how many cases have rectifications been undertaken? Were any Designated Authorities informed of the rectification and if so, which and when? *N/A*
(c) In how many cases have rectifications been denied and why they have been denied? *N/A*

40) See paragraph 39.
Have any complaints been made by individuals about CBP's handling of their PNR data?
No, none to date.
If so, how many? What was the respective complaint about? *N/A*

41) Have there been any complaints that were not resolved by CBP?
No complaints have been received to date.
If so,
(a) How many? In which cases could a complaint not be resolved? *N/A*
(b) In how many cases was a complaint directed to the Privacy Officer for review? How many complaints were resolved by such a review? In the case of no resolution, what was the complaint about? *N/A*

42) Have any complaints been referred to the DHS Privacy Office by DPAs in the EU on behalf of an EU resident to the extent such resident has authorised the DPA to act on his or her behalf and believes that his or her data-protection complaint regarding PNR has not been satisfactorily dealt with by CBP (as set out in paragraphs 37 to 41 of these undertakings) or the DHS Privacy Office?
No complaints have been received to date.
If so, how many? What were the complaints about? *N/A*
Has the DHS Chief Privacy Officer made any reports to Congress? If so, what do they say? *N/A*



EU PNR Policies

- CBP feels that Joint Reviews on an annual basis is appropriate at this time.
- CBP has published the "Undertakings" in the Federal Register.
- CBP has issued written policies for the use and disclosure of EU PNR data.
  - ➢Including specific guidance to FOIA personnel.
- CBP has placed policy warnings and reminders on the start-up screen of the system which maintains PNR data.

U.S. Customs and Border Protection

Undertaking #43-44

•FOIA and Privacy Act requests are handled by CBP through existing CBP procedures by way of mail, internet by e-mail, by telephone or they may hand deliver comment cards or make complaints to supervisors at the ports of entry.

•CBP has a dedicated unit that address all FOIAs and a separate unit that address inquiries and complaints. All FOIA requests, comments, complaints and responses are tracked.

•CBP has also developed procedures to specifically address FIOA requests pertaining to PNR issues and tracks them separately.

•Once a request is received from a data subject, if the information in a PNR is determined to be inaccurate, CBP will annotate the passenger's secondary examination record to reflect the inaccurate information.

• CBP has added an automated feature that would allow a note of the correct information to be linked to the appropriate PNR.

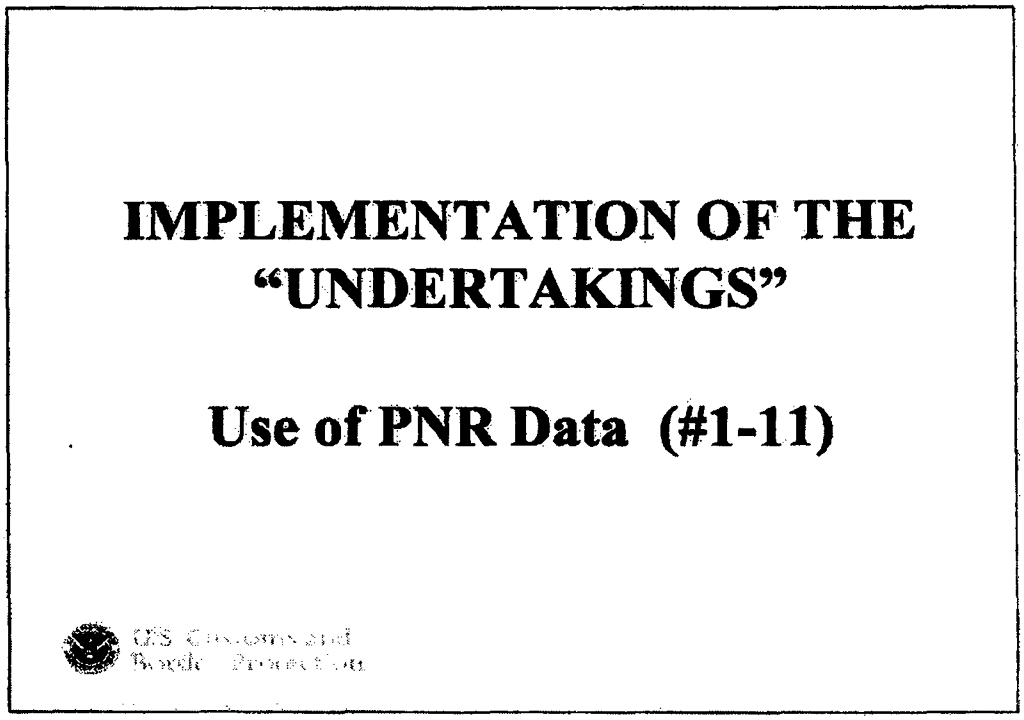
•CBP has established an automated disclosure log to better identify any Designated Authorities which have received such PNR data and notify them of any material that has been rectified.

Questions:
39) Have any requests been made to rectify data?
No, none to date.
If so,
(a) How many such requests have been made by passengers and crew members, air carriers or data protection authorities (DPAs) in the EU? Which data were concerned? *N/A*
(b) In how many cases have rectifications been undertaken? Were any Designated Authorities informed of the rectification and if so, which and when? *N/A*
(c) In how many cases have rectifications been denied and why they have been denied? *N/A*

40) See paragraph 39.
Have any complaints been made by individuals about CBP's handling of their PNR data?
No, none to date.
If so, how many? What was the respective complaint about? *N/A*

41) Have there been any complaints that were not resolved by CBP?
No complaints have been received to date.
If so,
(a) How many? In which cases could a complaint not be resolved? *N/A*
(b) In how many cases was a complaint directed to the Privacy Officer for review? How many complaints were resolved by such a review? In the case of no resolution, what was the complaint about? *N/A*

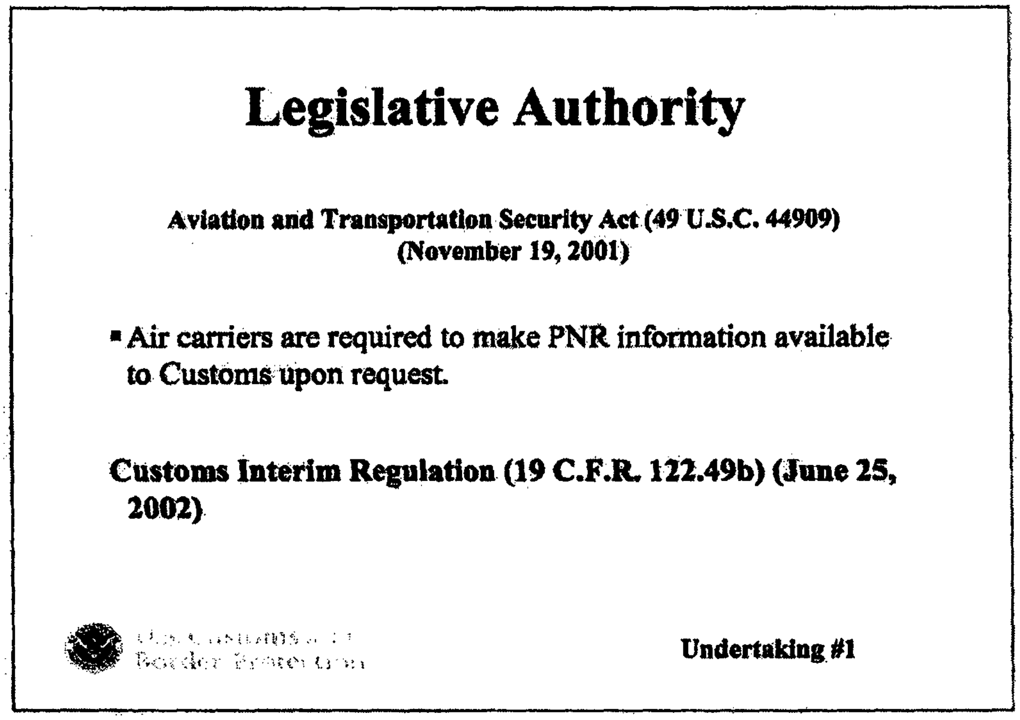
42) Have any complaints been referred to the DHS Privacy Office by DPAs in the EU on behalf of an EU resident to the extent such resident has authorised the DPA to act on his or her behalf and believes that his or her data-protection complaint regarding PNR has not been satisfactorily dealt with by CBP (as set out in paragraphs 37 to 41 of these undertakings) or the DHS Privacy Office?
No complaints have been received to date.
If so, how many? What were the complaints about? *N/A*
Has the DHS Chief Privacy Officer made any reports to Congress? If so, what do they say? *N/A*



IMPLEMENTATION OF THE "UNDERTAKINGS"

Use of PNR Data (#1-11)

U.S. Customs and Border Protection



Legislative Authority

Aviation and Transportation Security Act (49 U.S.C. 44909)
(November 19, 2001)

- Air carriers are required to make PNR information available to Customs upon request.

Customs Interim Regulation (19 C.F.R. 122.49b) (June 25, 2002)

U.S. Customs and
Border Protection

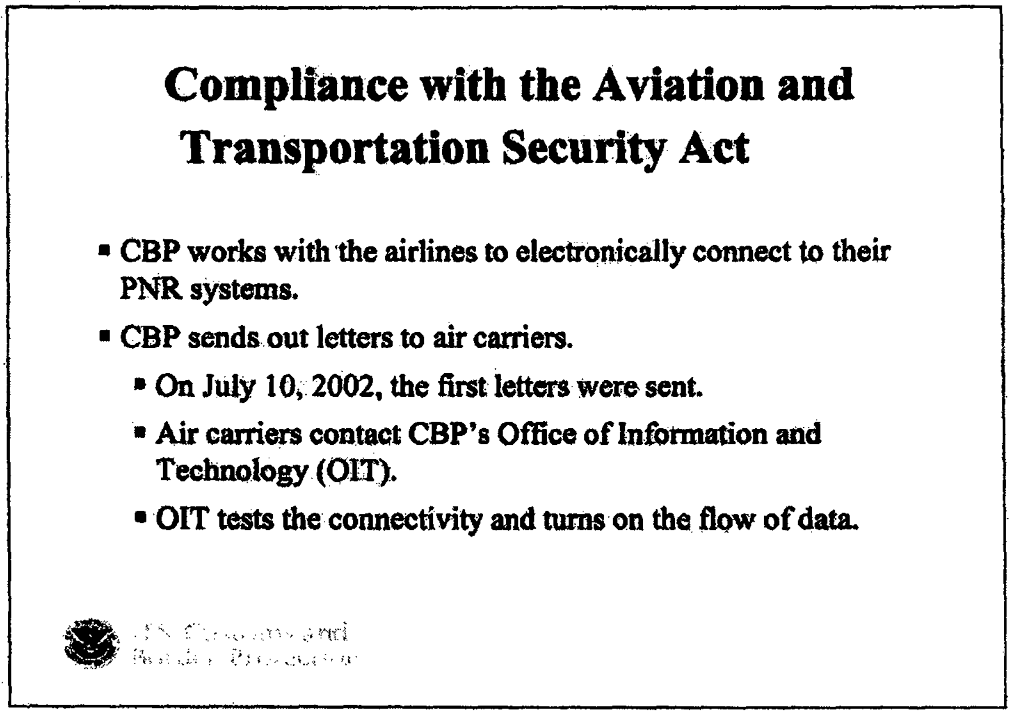
Undertaking #1

•On November 19, 2001, the President signed into law the Aviation and Transportation Security Act giving CBP the legislative authority to collect Advance Passenger Information (API) and Passenger Name Record (PNR) information from air carriers foreign and domestic, operating a passenger flight in foreign air transportation to the United States.

•Each air carrier, foreign and domestic operating a passenger flight in foreign air transportation to the United States must electronically transmit to Customs, in advance of the arrival of the flight, a related passenger manifest and a crew manifest containing certain required information pertaining to the passengers and crew on the flight.

•The purpose of this law is to support our priority mission of securing our nations borders and protecting national security.

•On June 26, 2002, CBP published an interim rule regarding CBP access to PNR information. This interim rule requires airlines to electronically connect their reservation and departure control systems to CBP within 30 days of receiving a written request.

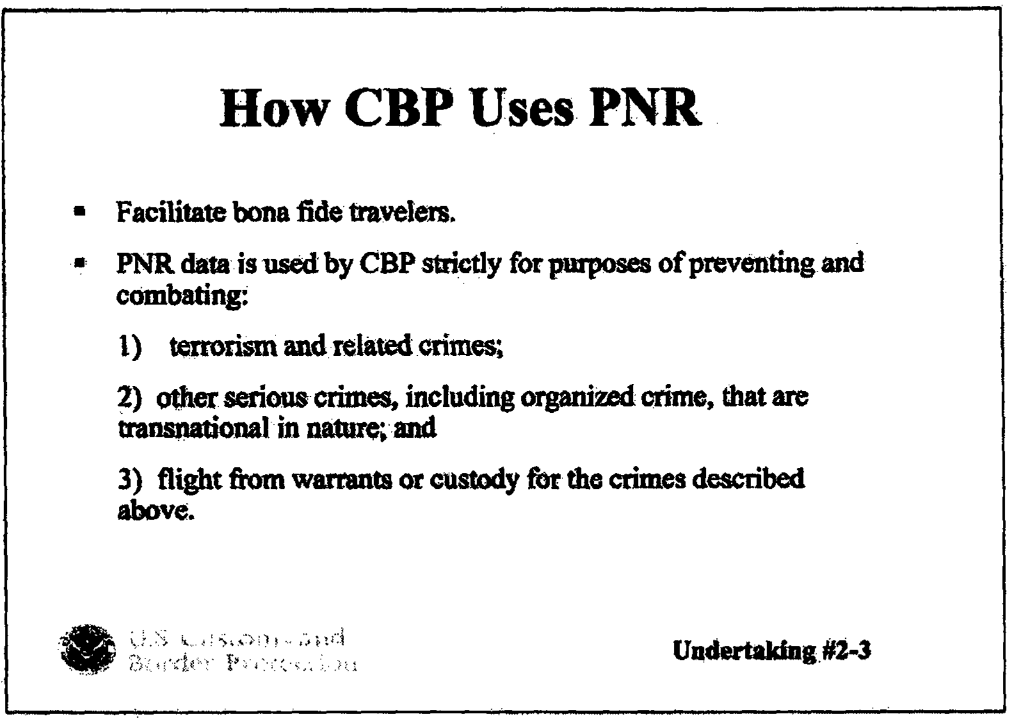


Compliance with the Aviation and Transportation Security Act

- CBP works with the airlines to electronically connect to their PNR systems.
- CBP sends out letters to air carriers.
  - On July 10, 2002, the first letters were sent.
  - Air carriers contact CBP's Office of Information and Technology (OIT).
  - OIT tests the connectivity and turns on the flow of data.

U.S. Customs and Border Protection

•It is CBP's longstanding responsibility to collect PNR data from all air carriers flying to and from the U.S., as provided by this U.S. law.



How CBP Uses PNR

- Facilitate bona fide travelers.
- PNR data is used by CBP strictly for purposes of preventing and combating:

  1) terrorism and related crimes;

  2) other serious crimes, including organized crime, that are transnational in nature; and

  3) flight from warrants or custody for the crimes described above.

U.S. Customs and Border Protection

Undertaking #2-3

•Most data elements contained in a PNR can be obtained by CBP upon examining a data subject's airline ticket and other travel documents pursuant to our normal border authority.

•The ability to receive PNR data electronically significantly enhances CBP's ability to facilitate *bona fide* travel and conduct efficient and effective advance risk assessment of passengers.

Questions:

3) What is the percentage of use of PNR for each of the three purposes mentioned above?

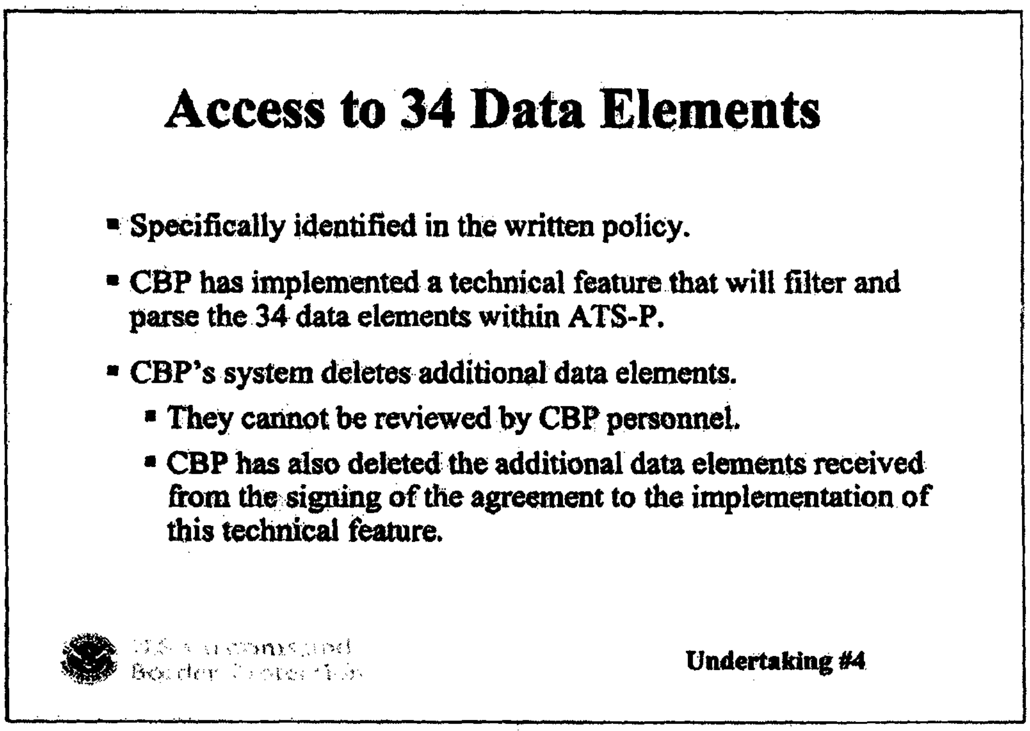
CBP is unable to quantify that specifically. Each PNR that is received by CBP is run through CBP systems to assess individual risk based on the identified purposes.

How does the current system assist in contributing to achieving each of the three purposes?

CBP to identify high-risk individuals (persons who may be involved in terrorism or related crimes, serious crimes that are transnational in nature, or are flights from warrants or custody related to such crimes) thereby allowing CBP to expedite the remaining travelers.

What is the provisional overall assessment of the use of PNR data re preventing and combating terrorism an organized crime? Does the system allow for a quicker clearance of bana fide travelers and if so, how much on average in real time?

DHS believes PNR is a critical tool in its efforts to identify persons of concern. Because CBP receives PNR and other passenger information in advance of flight's arrival, most primary inspections last only a minute or so and legitimate travelers are then allowed to proceed.



Access to 34 Data Elements

- Specifically identified in the written policy.
- CBP has implemented a technical feature that will filter and parse the 34 data elements within ATS-P.
- CBP's system deletes additional data elements.
  - They cannot be reviewed by CBP personnel.
  - CBP has also deleted the additional data elements received from the signing of the agreement to the implementation of this technical feature.

U.S. Customs and Border Protection

Undertaking #4

•CBP has issued written policy in the Field Guidelines, that include a list of the agreed upon 34 data elements in which authorized users are to use in their targeting efforts.

CBP has implemented technical features that parses the agreed upon 34 data elements directly from the air carrier's reservation system into ATS-P.

•Users are unable to view additional elements other than the 34 that is required, it is deleted in the same fashion as the sensitive data.

•In addition, CBP has deleted the EU PNR data is excess of the 34 data elements which were captured in CBP's system prior to implementation of the parsing and delete functions.

Questions:

4) Which data are stored?

Before PNR data derived from flights between the U.S. and the EU PNR data are stored by CBP, all terms exactly matching those in the "sensitive" code and "sensitive" term list are removed. Each PNR record is parsed to identify the 34 permitted, known field identifiers. The filtered and parsed data are stored in the data- base. Any other EU PNR data received from the host system is not stored by CBP.

Which data are transferred to CBP's own computer systems?

CBP receives raw EU PNR data from the hosting reservation system through a message queue. The raw data are not stored in any CBP computer system (see answer to data storage above).

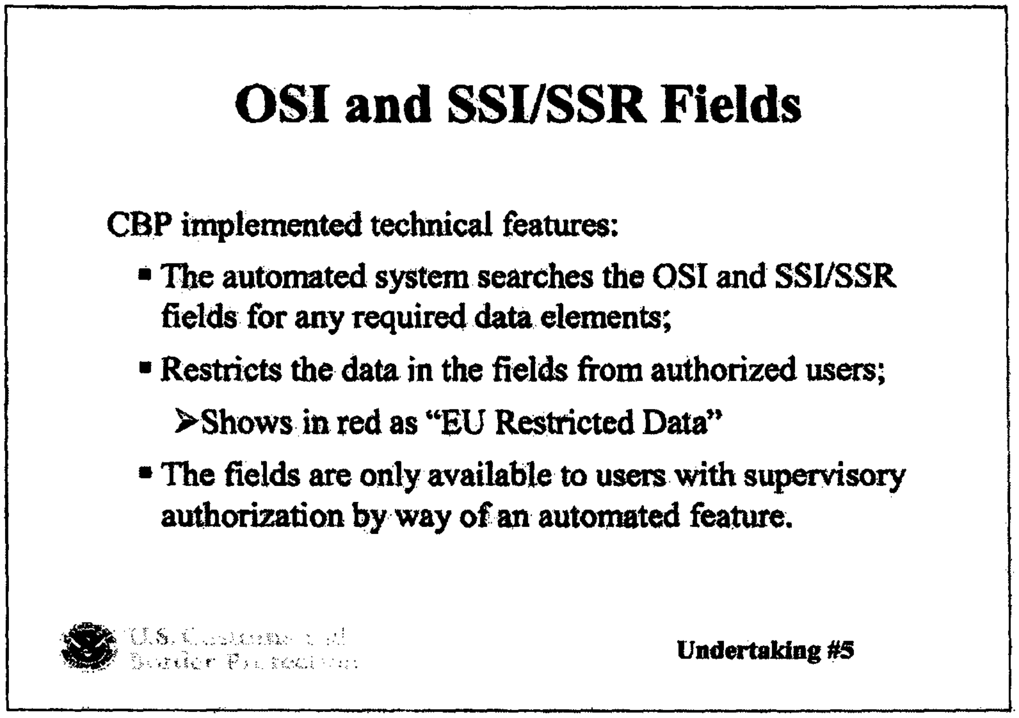
What is the volume of use of the 34 data elements, showing average number typically used, which have been used most and which were the fewest used elements?

CBP's system is designed to utilize all available data elements to better evaluate passengers, but the system does not track how often each element is in fact available in the system.

Has CBP become aware of any additional PNR data element that may be available and is of the view that the element is required for the purposes set out in paragraph 3? *No, not at this time.*

Has CBP become aware of any PNR element that is no longer required for the same purposes and if so, which element(s)?

No, CBP continues to need all available elements to better evaluate passengers. CBP intends to address this issue further during our presentation.



OSI and SSI/SSR Fields

CBP implemented technical features:

- The automated system searches the OSI and SSI/SSR fields for any required data elements;
- Restricts the data in the fields from authorized users;
  - ➢Shows in red as "EU Restricted Data"
- The fields are only available to users with supervisory authorization by way of an automated feature.

U.S. Customs and Border Protection

Undertaking #5

Explain:

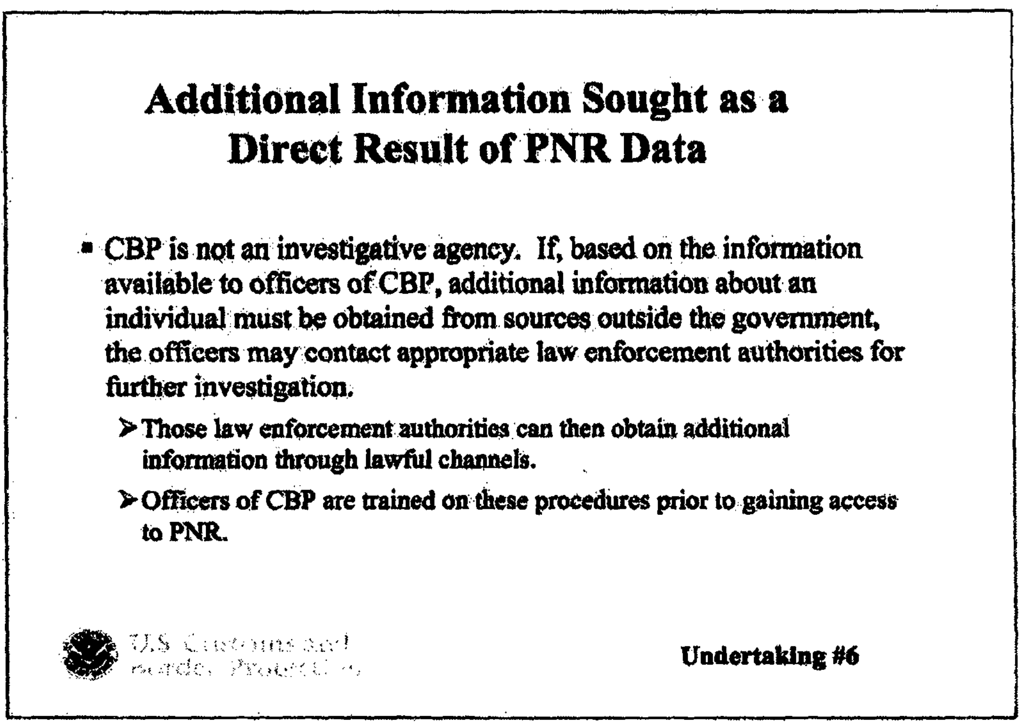
•The written policy includes notification that fields will be blocked by CBP's system to prevent viewing by authorized users.

•In the event that the subject of a PNR is identified as high-risk, an authorized supervisors can grant authorization to the user to open the fields, by way of an automated feature.

Questions:

5) Have any manual reviews of 'OSI' and 'SSI/SSR' fields been made? If so, in how many cases?

Yes, CBP has manually accessed a small percentage of these fields and looks forward to addressing this issue in more detail during the joint review.



Additional Information Sought as a Direct Result of PNR Data

- CBP is not an investigative agency. If, based on the information available to officers of CBP, additional information about an individual must be obtained from sources outside the government, the officers may contact appropriate law enforcement authorities for further investigation.
  - ➢ Those law enforcement authorities can then obtain additional information through lawful channels.
  - ➢ Officers of CBP are trained on these procedures prior to gaining access to PNR.

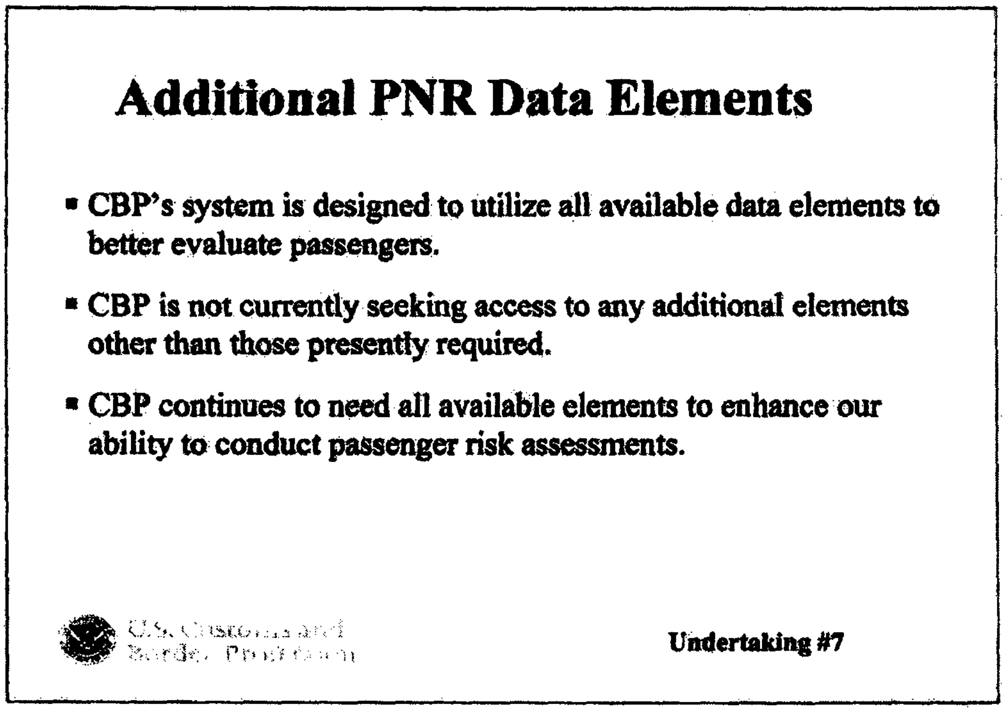
U.S. Customs and Border Protection

Undertaking #6

•CBP would obtain additional information as a direct result of a PNR, but CBP is not an investigative agency, if further investigation or obtaining additional information is required (such as obtaining transaction information from a credit card listed in a PNR) CBP would forward the case to the appropriate law enforcement authorities, such as DHS ICE for follow-up.

6) Have there been cases where additional personal information was obtained from outside? If so, in how many cases? Which type of personal information has been obtained, from where has it been obtained, and which channels have been used?

Current law and applicable policies would require CBP and other U.S. authorities to comply with the substance of this provision. CBP is not an investigative agency, therefore, generally, when further investigation is required (which would include the obtaining of additional information), the case is forwarded to the appropriate law enforcement authorities, such as DHS Immigration and Customs Enforcement (ICE), for follow-up. Further information will be offered during the joint review.



Additional PNR Data Elements

- CBP's system is designed to utilize all available data elements to better evaluate passengers.
- CBP is not currently seeking access to any additional elements other than those presently required.
- CBP continues to need all available elements to enhance our ability to conduct passenger risk assessments.

U.S. Customs and Border Protection

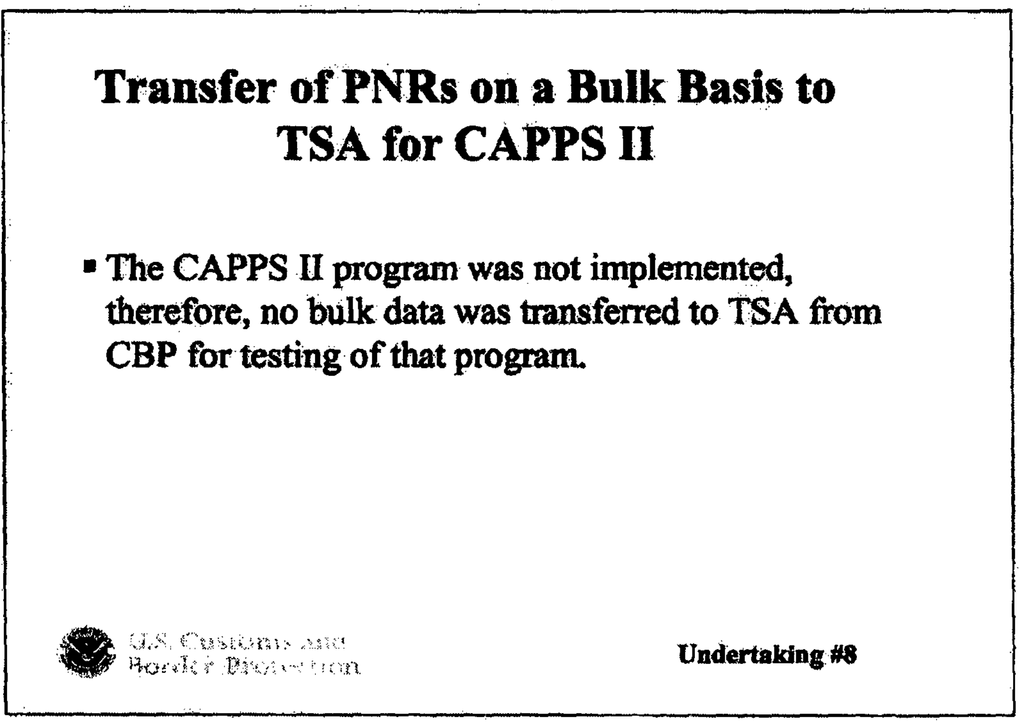
Undertaking #7

Questions:

7) Consultation with the Commission regarding revision of the required PNR data elements, prior to effecting any such revision.

CBP has not become aware of any additional PNR data element that may be available or required for the purposes set out in paragraph 3.

CBP continues to need all available elements to better evaluate passengers. CBP intends to address this issue further during our presentation.



Transfer of PNRs on a Bulk Basis to TSA for CAPPS II

- The CAPPS II program was not implemented, therefore, no bulk data was transferred to TSA from CBP for testing of that program.

U.S. Customs and Border Protection

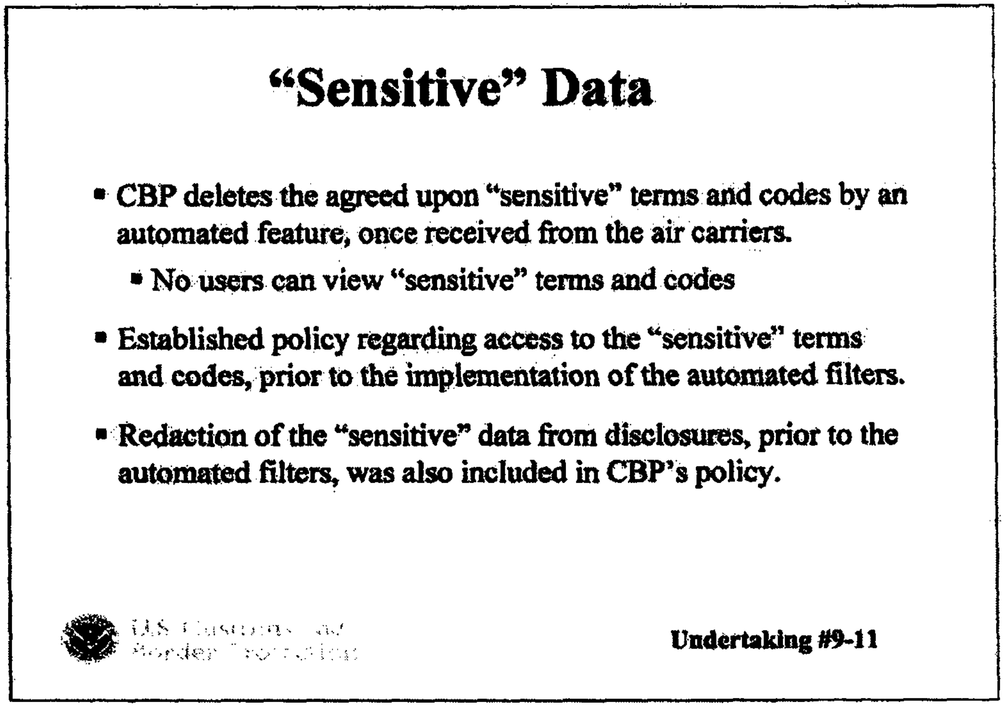
Undertaking #8

Question:
8) Was data ever transferred for testing? If so, was it filtered? Was it used in an emergency situation?
Has data on European flights by US airlines been used for testing?

No. The CAPPS II program was not implemented, therefore, no data was transferred to TSA for testing of said program.

Is PNR data planned to be transferred to/already being transferred to TSA for the purposes of testing Secure Flight?

No. PNR data was not transferred, and there are no plans to transfer PNR data to TSA for purposes of testing Secure Flight.



“Sensitive” Data

- CBP deletes the agreed upon “sensitive” terms and codes by an automated feature, once received from the air carriers.
  - No users can view “sensitive” terms and codes
- Established policy regarding access to the “sensitive” terms and codes, prior to the implementation of the automated filters.
- Redaction of the “sensitive” data from disclosures, prior to the automated filters, was also included in CBP’s policy.

Undertaking #9-11

Explain:

•On October 14, 2004, CBP received an informal approval of the “sensitive” list of terms and codes to be filtered. On October 27, 2004, CBP began finalizing the draft copy of the User Requirements to make the necessary changes within our system. On March 18, 2005, CBP was able to implement the sensitive data filters and it was done “ with the least possible delay.”

•The agreed upon “sensitive” terms and codes are deleted by an automated feature, once received from the air carriers and before transferred into our system. No users can view “sensitive” terms and codes and anytime.

•CBP established a written policy that lists the agreed upon “sensitive” terms and codes and instruct authorized users that the terms and codes should not be used in targeting efforts, pending the automated filters.

•CBP also issued policy regarding the redaction of the “sensitive” data, prior to the implemenation of the automated filters.

•The policy regarding the redaction of sensitive data before properly disclosing EU PNR data is also included in the field guidance. CBP at HQ keeps a file of all disclosures.

•CBP has established policies (Table of Offenses and Standards of Conduct) that prevent the use of any “sensitive” information (such as race, sex, religion, etc.) in official duties as well as penalties for such action.

Questions:

9) Mainly descriptive, obligations are specified in §§ 10 and 11.

Has sensitive data ever been used?

No, no cases of use of “sensitive” data, inconsistent with the Undertakings, have been reported to date. CBP has conducted extensive training in an effort to prevent such use prior to implementation of the filters (see response to paragraph 10 below).

Does CBP use sensitive data concerning European flights accessed from US’ airlines CRS?

See above.

10) When has the filtering system been implemented?

The filtering functionality for EU PNR “sensitive” codes and terms was implemented in March 2005.

Does it concern PNR data filtering and filtering of sensitive data including free text or open fields?

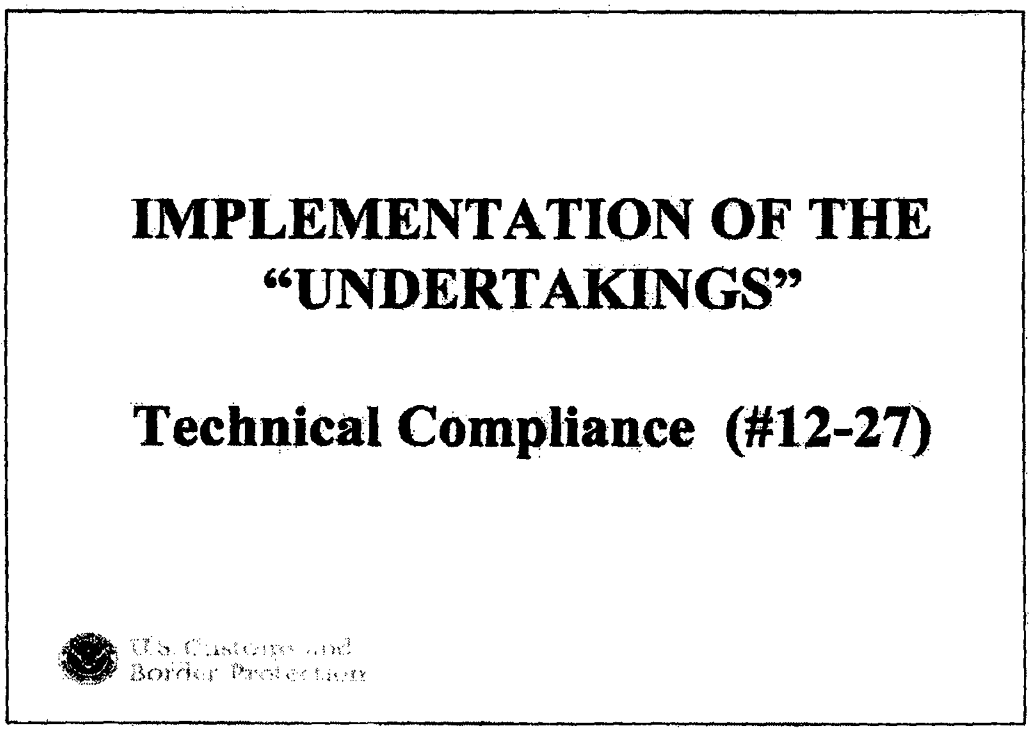
Yes.

Does it filter out flights from the EU not destined to the US?

CBP’s system is programmed to limit automated pulls to only PNR associated with flights between the U.S. and EU (flights from the EU with no U.S. nexus are not subject to the automated pulls).

Does it encounter problems, for example filtering of open fields?

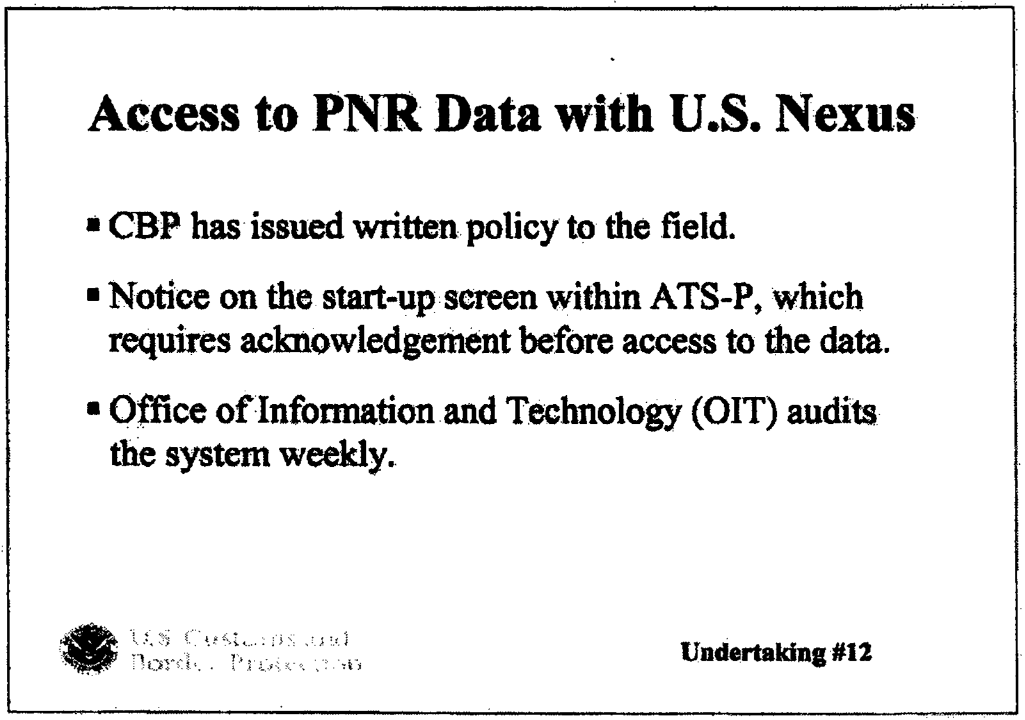
To date, there have been no operational problems involved with sensitive code or term



IMPLEMENTATION OF THE "UNDERTAKINGS"

Technical Compliance (#12-27)

U.S. Customs and
Border Protection



Access to PNR Data with U.S. Nexus

- CBP has issued written policy to the field.
- Notice on the start-up screen within ATS-P, which requires acknowledgement before access to the data.
- Office of Information and Technology (OIT) audits the system weekly.

U.S. Customs and Border Protection

Undertaking #12

Explain:

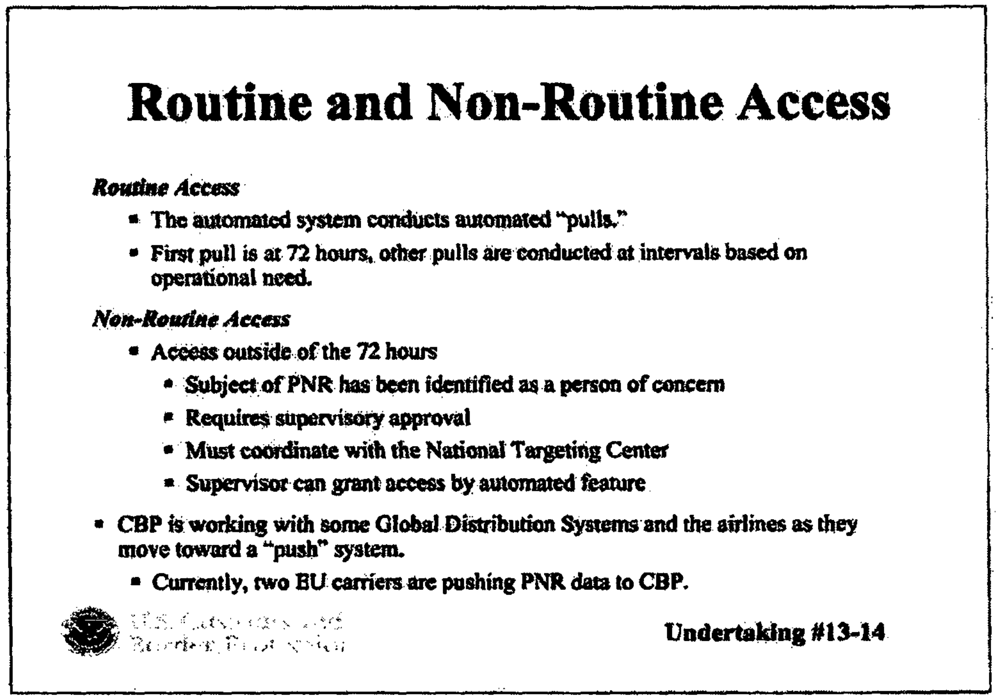
•CBP has issued written policies to the field that restricts access to only PNR data with U.S. nexus.

•There is a notice on the start-up screen in ATS-P, which requires that they click a button that acknowledges the restrictions before they are able to access the data.

•OIT audits the system weekly and reports any violations to the Executive Director, Border Security and Facilitation.

•To date no violations of EU PNR have been reported.

High (b)(2) /(b)(7)(E)
(b)(5)



Routine and Non-Routine Access

Routine Access

- The automated system conducts automated "pulls."
- First pull is at 72 hours, other pulls are conducted at intervals based on operational need.

Non-Routine Access

- Access outside of the 72 hours
  - Subject of PNR has been identified as a person of concern
  - Requires supervisory approval
  - Must coordinate with the National Targeting Center
  - Supervisor can grant access by automated feature
- CBP is working with some Global Distribution Systems and the airlines as they move toward a "push" system.
  - Currently, two EU carriers are pushing PNR data to CBP.

Undertaking #13-14

<u>Explain:</u>
Access to PNR data is broken into two parts routine and non-routine.

•Routine access is when the ATS-P system conducts automated "pulls."

•First pull is at 72 hours, others are based on operational need.

•To better regulate the three required pulls that are automated, CBP has restricted access to pulling EU PNR data. The supervisor may authorize access to do a manual pull to authorized users by an automated feature.

•Non-routine access is when a subject of a PNR has been identified as a person of concern, upon supervisory approval and coordination with the NTC, CBP will manually pull PNR data, if deemed necessary

•CBP has established an automated feature in which supervisors may grant approval before an manual pull is made.

•CBP members at the NTC maintains a manual log of the "manual" pulls.

•CBP is working diligently with some Global Distributing Systems and the airlines as they move to a "push" system.

•Currently, two EU carriers are pushing PNR data to CBP. (Austrian and Aer Lingus)

Questions:

13) What preparations is CBP making in order to be able to receive pushed data from EU carriers / centralised reservation systems?

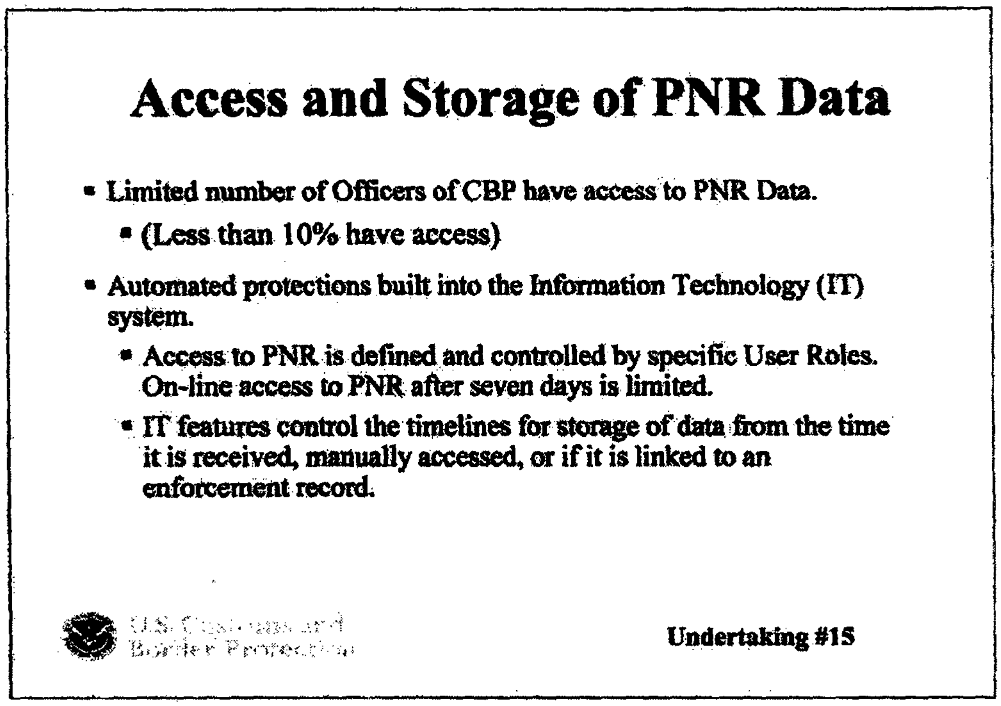
The TCP/IP infrastructure between host systems to handle expected capacity of PNR data has been deployed. DHS is actively engaged in discussions with the airline industry regarding the design of a push system and is currently receiving push data from some airlines.

14) Have there been cases where PNR data have been pulled or pushed prior to 72 hours before departure and through which channels?

If so, in how many cases?

How many times particular details have been accessed?

Yes, CBP has pulled a small percentage of PNR data prior to 72 hours in compliance with the Undertakings, and looks forward to addressing these issues during the joint review.



Access and Storage of PNR Data

- Limited number of Officers of CBP have access to PNR Data.
  - (Less than 10% have access)
- Automated protections built into the Information Technology (IT) system.
  - Access to PNR is defined and controlled by specific User Roles. On-line access to PNR after seven days is limited.
  - IT features control the timelines for storage of data from the time it is received, manually accessed, or if it is linked to an enforcement record.

U.S. Customs and Border Protection

Undertaking #15

Explain:

•A limited number of CBP Officer have access to PNR data. Less than 10% have access.

•The Field Guidelines advises that PNR data will be limited to certain authorized personnel of the PAUs and NTC personnel after seven days.

•Access to PNR is defined and technically controlled by specific User Roles helps limit access to the PNR data and

High (b)(2)/(b)(7)(E)

•There are approximately 1142 CBP employees with access to PNR data. After the seven days that number is reduced by 467, which equals out to 1.6% of CBP personnel with this access.

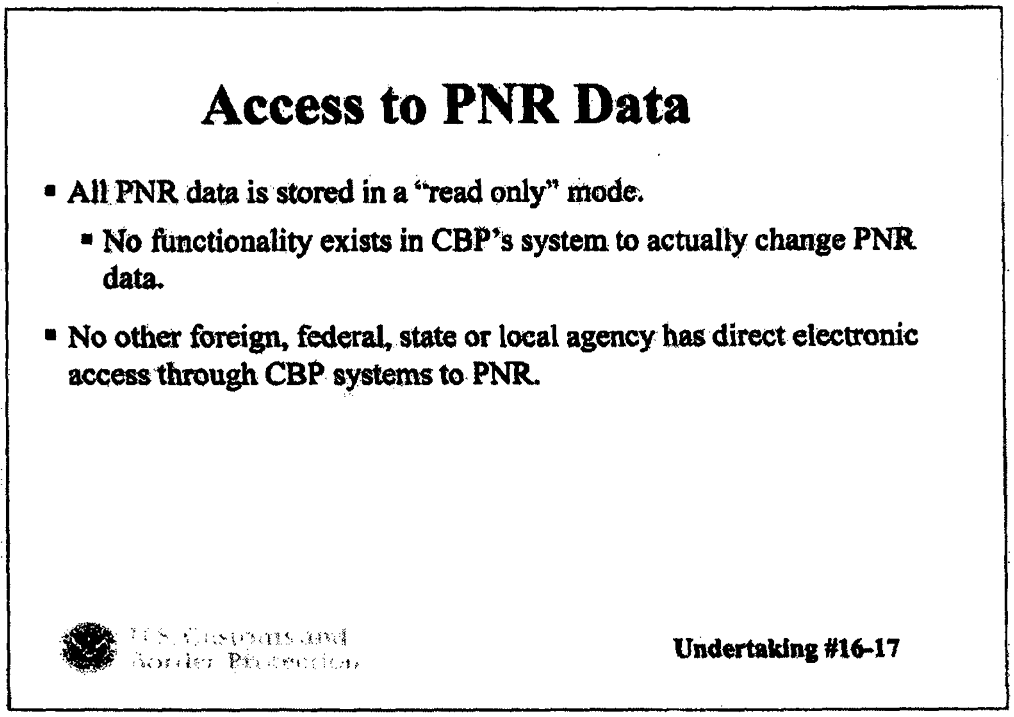
•IT features also define and control the timelines for storage of data from the time it is received by CBP.

•The IT features also determines which data that has been manually accessed and applies the appropriate storage time, as well as data that has been linked to an enforcement record.

Questions:

15) What measures have been taken to restrict access only to authorised CBP users at each stage?

Through an automated process, access is limited on an individual basis (defined "user roles"), depending upon the specific duties of an officer. CBP will provide more specific details during the joint review.



Access to PNR Data

- All PNR data is stored in a "read only" mode.
  - No functionality exists in CBP's system to actually change PNR data.
- No other foreign, federal, state or local agency has direct electronic access through CBP systems to PNR.

U.S. Customs and Border Protection

Undertaking #16-17

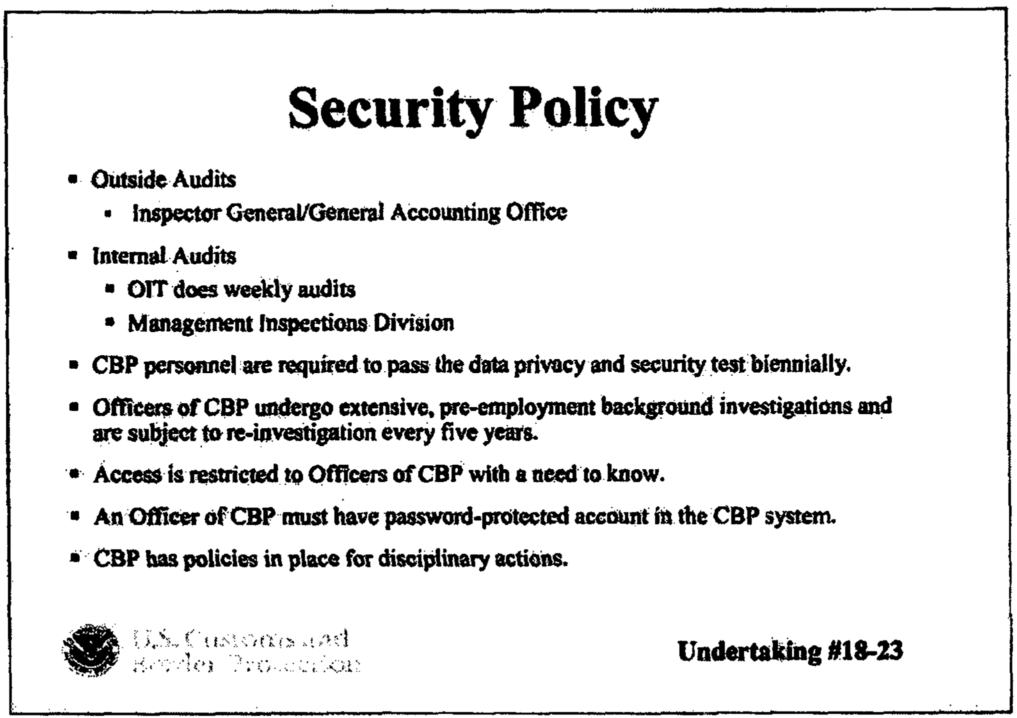
<u>Explain:</u>
•As demonstrated at the site visit, all PNR data is stored as 'read only' mode.

•All users identified by their user roles with access to PNR data have the "need to know" and support the mission of safeguarding our borders.

•No functionality exists in CBP systems to actually change PNR data, but there are mechanisms in place to note any necessary corrections to the data as demonstrated at your site visit.

Questions:
16) Visit of the operations taking place at a terminal at an airport and at CBP's premises re security measures. How many staff has 'read only' access?
What are their job roles? How is access restricted in case of 'read only'?
All PNR data is stored in "Read Only" mode. No functionality exists in CBP systems to actually change PNR data, but there are mechanisms in place to note any necessary corrections to the data. CBP will address issues related to the roles of officers who have access to PNR in its system during the joint review.

17) *No other agency has direct access to PNR that CBP obtains pursuant to 49 U.S.C. 44909 and stores in its systems consistent with the Undertakings.*



Security Policy

- Outside Audits
  - Inspector General/General Accounting Office
- Internal Audits
  - OIT does weekly audits
  - Management Inspections Division
- CBP personnel are required to pass the data privacy and security test biennially.
- Officers of CBP undergo extensive, pre-employment background investigations and are subject to re-investigation every five years.
- Access is restricted to Officers of CBP with a need to know.
- An Officer of CBP must have password-protected account in the CBP system.
- CBP has policies in place for disciplinary actions.

U.S. Customs and Border Protection

Undertaking #18-23

Explain:
•Outside Audits – Inspector General/General Accounting Office

•Internal Audits

• Details regarding access to information in CBP databases are automatically recorded by OIT.
•OIT also does audit weekly for unauthorized access to PNR data without a U.S. nexus.

•Management Inspections Division

•Management Inspections & Integrity Assurance (formerly Internal Affairs) will perform routine audits of the system for unauthorized use.
•No reports of unauthorized use of EU PNR data has been reported.

•CBP personnel are required to pass the data privacy and security test biennial to maintain access to CBP's systems.
•This test is automated, if the test is not taken or passed the access to the system will be lost automatically.

•Access is restricted to CBP Officers with a need to know. Majority of the access is given to the members of the Passenger Analysis Units and the members at the National Targeting System.

(b)(2)/
(b)(7)(E)

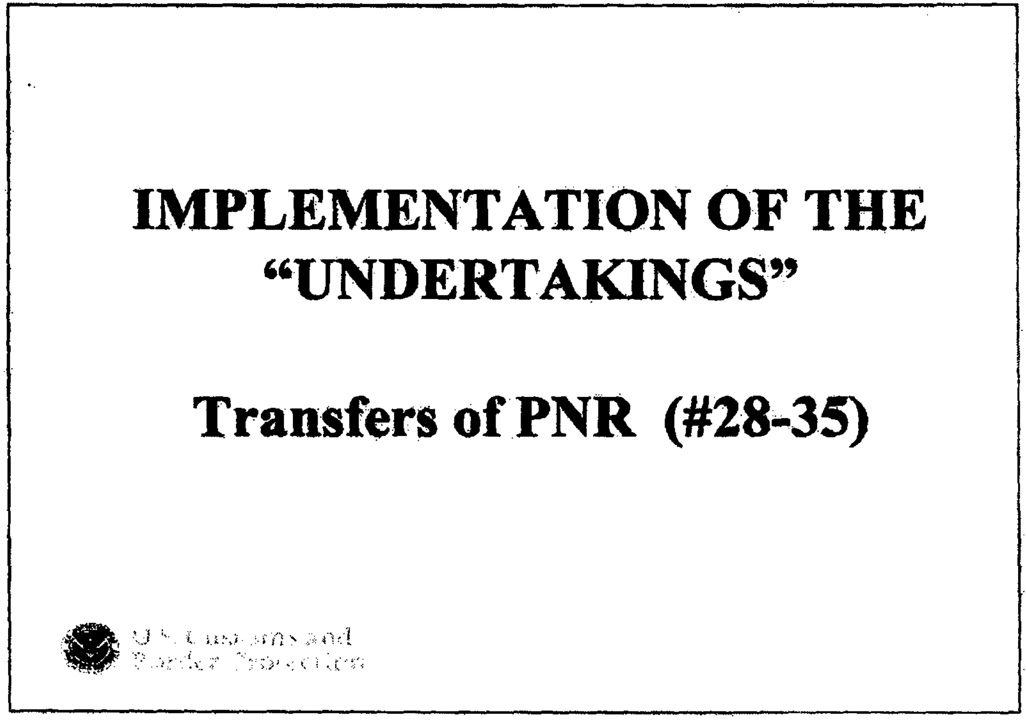
•Again approximately personnel has access to PNR data.

•CBP is unable to provide copies of audits, but is able express with fortitude that CBP has been using PNR data since 1992 without any problems.

•To date, there has been no reports of unauthorized access or unauthorized disclosures of EU PNR data.

Questions:
18) Any available copies of records and audits.
How many audits have been undertaken?
CBP looks forward to addressing this issue during the joint review.

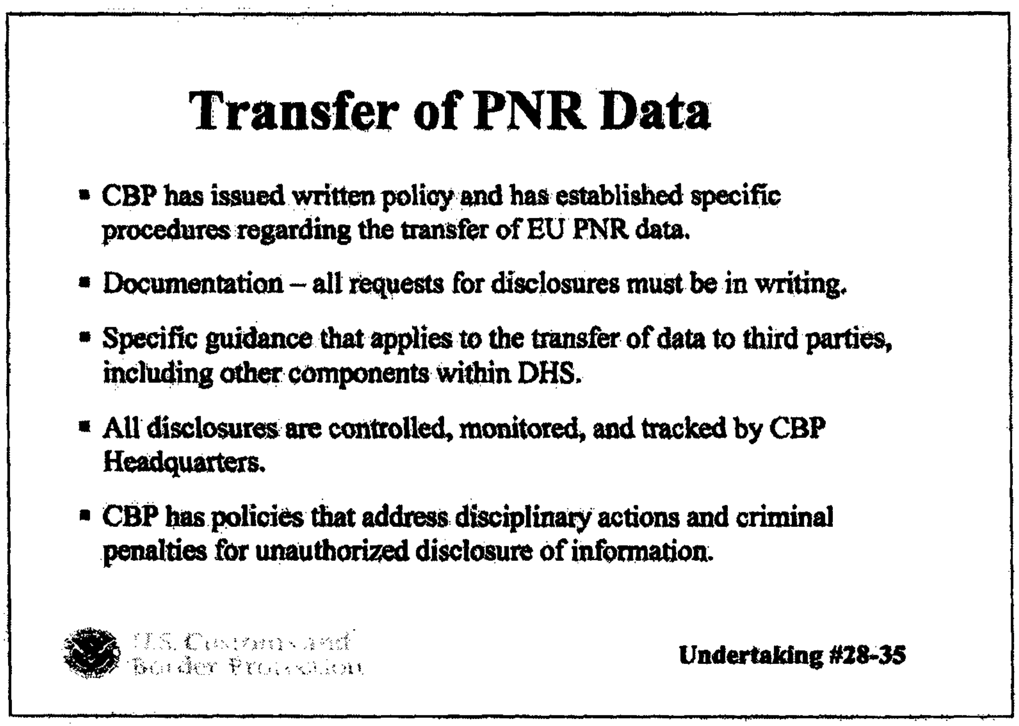
19) See paragraph 16.
All CBP personnel have received background investigations, consistent with applicable federal executive branch standards and requirements.
In addition information on numbers of officers, employees and contractors concerned.
As noted above all of CBP personnel have received background investigations. CBP anticipates providing more detailed numbers during the joint review.
20) Any available copies of audits and general information on the security and data privacy training.
Training regarding system security and data privacy is required before access to the system is granted and on a regular basis thereafter.
Has training on security and/or data privacy been provided?
Yes, same as above.
If so, how many CBP personnel took part in this training?



IMPLEMENTATION OF THE "UNDERTAKINGS"

Transfers of PNR (#28-35)

U.S. Customs and
Border Protection



Transfer of PNR Data

- CBP has issued written policy and has established specific procedures regarding the transfer of EU PNR data.
- Documentation – all requests for disclosures must be in writing.
- Specific guidance that applies to the transfer of data to third parties, including other components within DHS.
- All disclosures are controlled, monitored, and tracked by CBP Headquarters.
- CBP has policies that address disciplinary actions and criminal penalties for unauthorized disclosure of information.

U.S. Customs and Border Protection

Undertaking #28-35

- CBP has issued policy in the Field Guidelines regarding proper disclosure procedures to other U.S or foreign government agencies.
- Final requests are to be in writing from eligible authorities consistent with the purposes identified and specific forms to be filled out before or immediately after a disclosure takes place.
- The Guidelines provide information regarding other DHS components are to be treated as a "third party agencies."
- It also entails that PNR can only be provided to other U.S. or foreign government authorities with counter-terrorism or law enforcement functions and on a case-by-case basis.
- The Guidelines also instruct authorized personnel to redact any "sensitive" data as reference in the agreed upon "sensitive" terms and codes before implementing the automated filters.
- CBP HQ reviews and keeps a file of all disclosures. Currently, approximately ?? disclosures have been made since November 2003.
- Disclosures of various PNR data have been made to other government authorities such as ICE , TSA and FBI. Some instances only passenger lists have been given, individual PNRs, or confirmation that someone is on a flight or arriving on a certain date.
- CBP has not disclosed any information to any foreign authorities.
- CBP has policies that address disciplinary actions and criminal penalties for unauthorized disclosure of information. To date, no reports of unauthorized disclosures have been made.

Questions:

28) See paragraph 29.

CBP looks forward to addressing this issue during the joint review.

29) In how many cases PNR data have been transferred to other government authorities? To which authorities have the respective PNR data been transferred? Which PNR data have been transferred?

CBP is in compliance with the Undertakings and looks forward to providing more specific details during the joint review. Generally CBP does not transfer PNR data. However, CBP does share the results of specific case analysis (without PNR data record) with Law Enforcement Agencies.

30) Copies of some cases, if any.

What procedures are in place to determine whether the disclosure fits within the agreed purposes?

CBP has issued policies, which reflect the representations of the Undertakings. Copies of information related to any disclosures are routinely sent to CBP headquarters to verify compliance with these policies and maintain centralized records. CBP will provide further information regarding these processes during its presentations.

31) To what extent CBP is satisfied with the way the obligation set out in §§ 31 and 32 have been respected by other Designated Authorities?

CBP has always placed conditions upon the information, which it discloses to other government authorities and is satisfied that such conditions, including those specific to EU PNR, have been respected by such authorities.

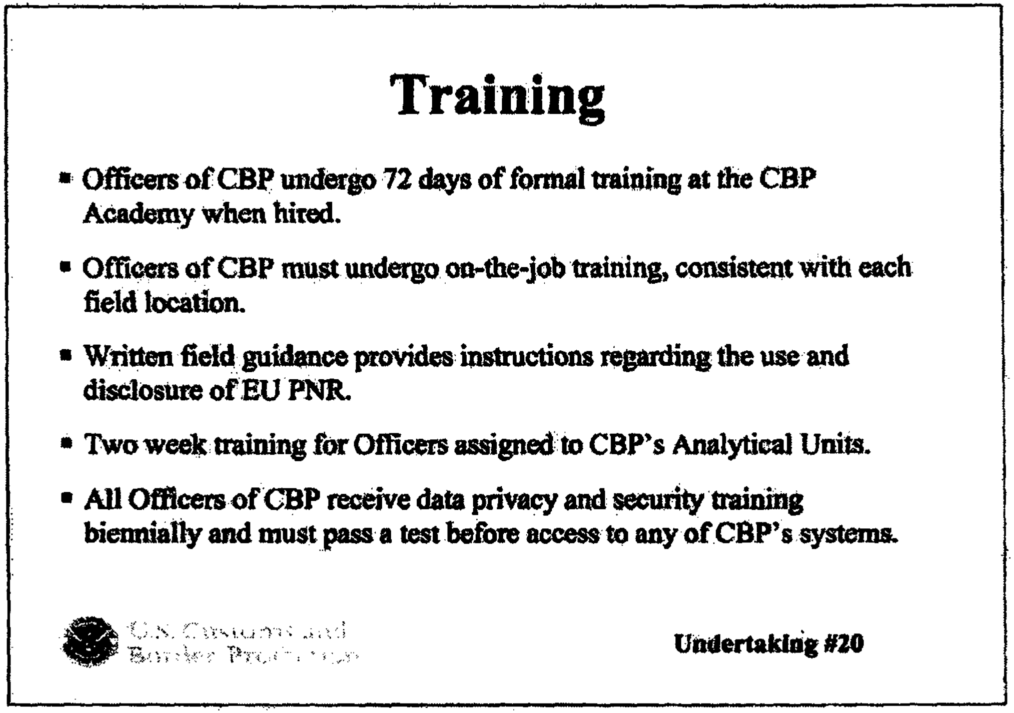
Have cases been reported to the DHS Chief Privacy Officer? If so, has any action been taken and of which nature? *No cases of other government authorities failing to comply with these conditions have been reported to date.*

32) See paragraph 31.

See response to paragraph 31.

33) (a) Have there been cases of unauthorised disclosure of PNR data by persons employed in other government authorities?

No cases have been reported to date.



Training

- Officers of CBP undergo 72 days of formal training at the CBP Academy when hired.
- Officers of CBP must undergo on-the-job training, consistent with each field location.
- Written field guidance provides instructions regarding the use and disclosure of EU PNR.
- Two week training for Officers assigned to CBP's Analytical Units.
- All Officers of CBP receive data privacy and security training biennially and must pass a test before access to any of CBP's systems.

U.S. Customs and Border Protection

Undertaking #20

•The written field guidance provide significant training regarding the use and disclosure of all aspects of EU PNR. Employees must sign off and input receipt into 'o track and confirm receipt.

(b)(2)/(b)(7)(E)

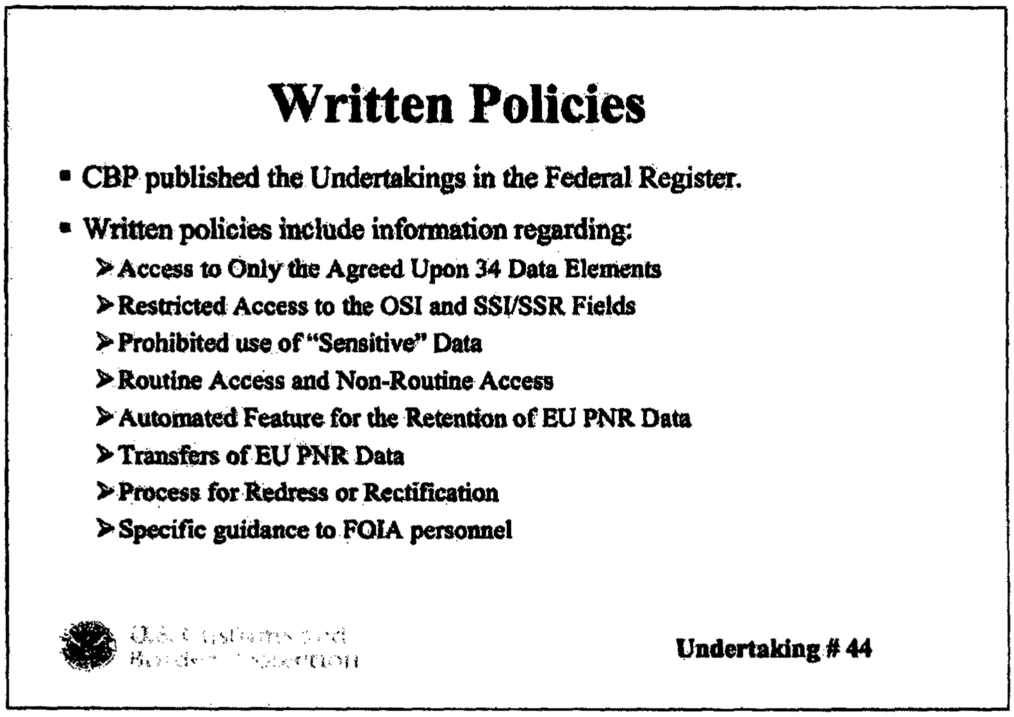
•When assigned to field Analytical units, employees attend two week analytical training that highlight the use of CBP's various databases and how to conduct effective targeting.

•Training of EU PNR has also been added to that formal training, regarding the restrictions of the use of that data, as well as the disclosure procedures.

•Again, all CBP employees must receive data privacy and security training that is taken biennial for continued access to CBP's systems.

Undertaking #20

CBP Officers, employees and contractors are required to complete security and data privacy training, including passage of a test, on a biennial basis.



Written Policies

- CBP published the Undertakings in the Federal Register.
- Written policies include information regarding:
  - ➢Access to Only the Agreed Upon 34 Data Elements
  - ➢Restricted Access to the OSI and SSI/SSR Fields
  - ➢Prohibited use of "Sensitive" Data
  - ➢Routine Access and Non-Routine Access
  - ➢Automated Feature for the Retention of EU PNR Data
  - ➢Transfers of EU PNR Data
  - ➢Process for Redress or Rectification
  - ➢Specific guidance to FOIA personnel

Undertaking # 44

Explain:

•As previously mentioned, CBP published the Undertakings in the Federal Register.

•CBP issued written policy on December 20, 2004, to address the access, use, and disclosure of PNR information to the field.

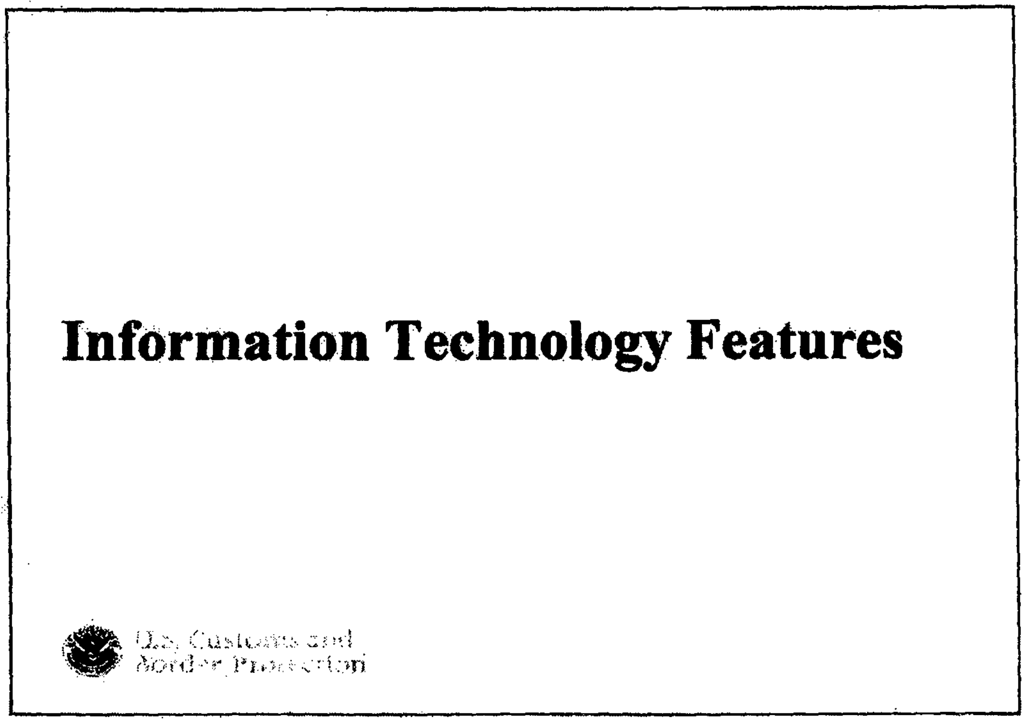
•This written policy includes the following information:

•This policy superceded the "interim guidance to the field" issued in July 2003.

Questions:

43-44) What regulations, directives or other policy documents have been adopted? See paragraphs 21-32.

CBP has issued a policy regarding the use and disclosure of EU PNR, and has published the Undertakings in the Federal Register. CBP will provide more specific information regarding this issue during the joint review.



Information Technology Features

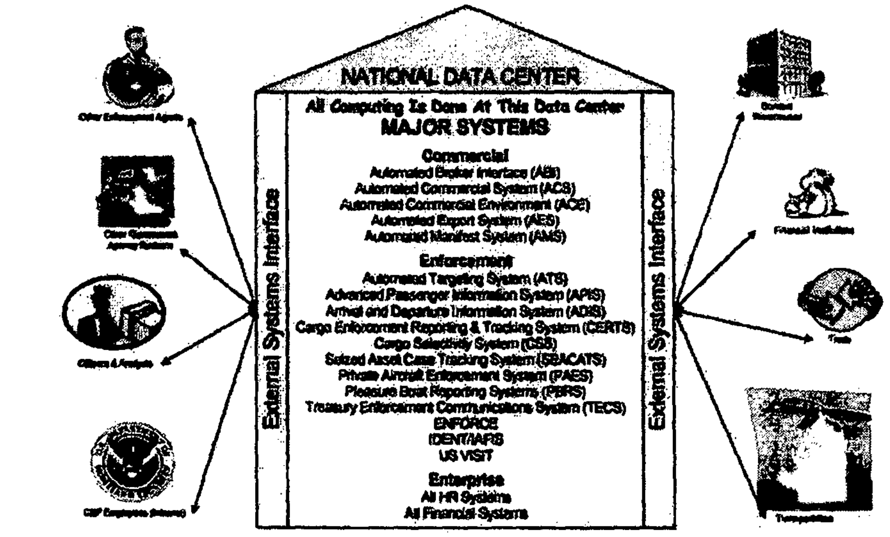
U.S. Customs and
Border Protection

The next part of the presentation will illustrate the information and technology features that CBP added to implement the "Undertakings."

[introduction]

I am going to tell you about the IT organization who implemented the undertakings, the procedures we followed, and then explain how the automated features work.

CBP National Data Center



NATIONAL DATA CENTER

All Computing Is Done At This Data Center

MAJOR SYSTEMS

Commercial

Automated Broker Interface (ABI)
Automated Commercial System (ACS)
Automated Commercial Environment (ACE)
Automated Export System (AES)
Automated Manifest System (AMS)

Enforcement

Automated Targeting System (ATS)
Advanced Passenger Information System (APIS)
Arrival and Departure Information System (ADIS)
Cargo Enforcement Reporting & Tracking System (CERTS)
Cargo Selectivity System (CSS)
Seized Asset Case Tracking System (SEACATS)
Private Aircraft Enforcement System (PAES)
Pleasure Boat Reporting Systems (PBRS)
Treasury Enforcement Communications System (TECS)
ENFORCE
IDENT/IAFS
US VISIT

Enterprise

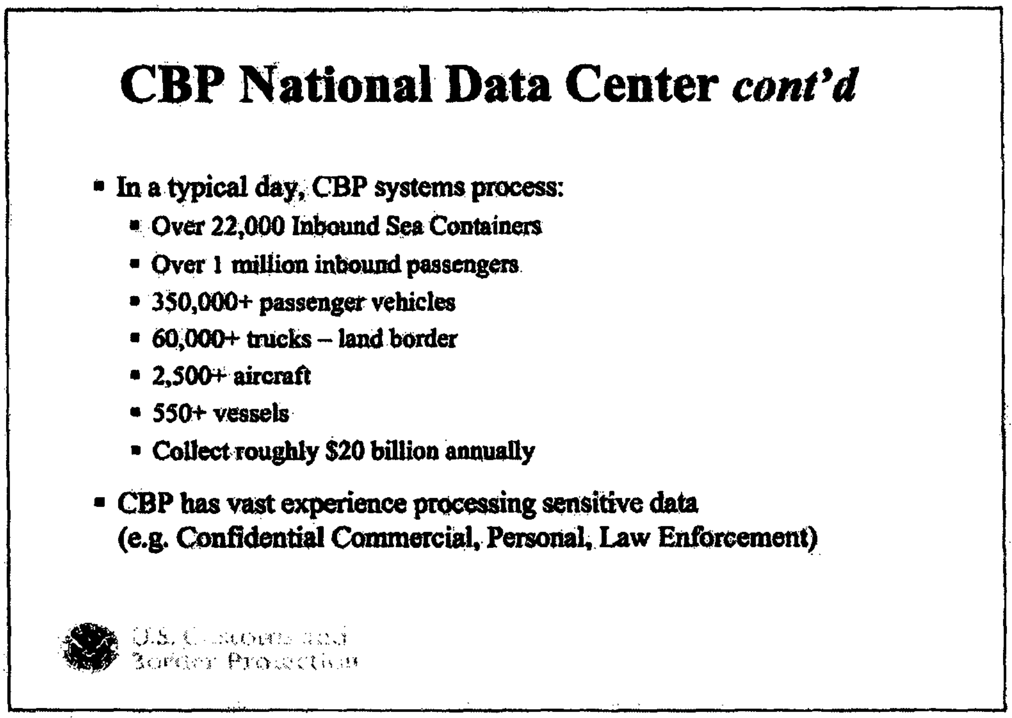
All HR Systems
All Financial Systems

U.S. Customs and
Border Protection

Largest DHS Data Center, and 2nd Largest Federal Civilian Data Center
Technology, size, and complexity similar to a Fortune 100 company – e.g., UPS, FedEx

Interfaces with:

- Over 2000 financial institutions
- Over 2000 Trade Partners
- Over 90 airlines
- Most major Government departments and many agencies and bureaus



CBP National Data Center *cont'd*

- In a typical day, CBP systems process:
  - Over 22,000 Inbound Sea Containers
  - Over 1 million inbound passengers
  - 350,000+ passenger vehicles
  - 60,000+ trucks – land border
  - 2,500+ aircraft
  - 550+ vessels
  - Collect roughly $20 billion annually
- CBP has vast experience processing sensitive data (e.g. Confidential Commercial, Personal, Law Enforcement)

U.S. Customs and Border Protection

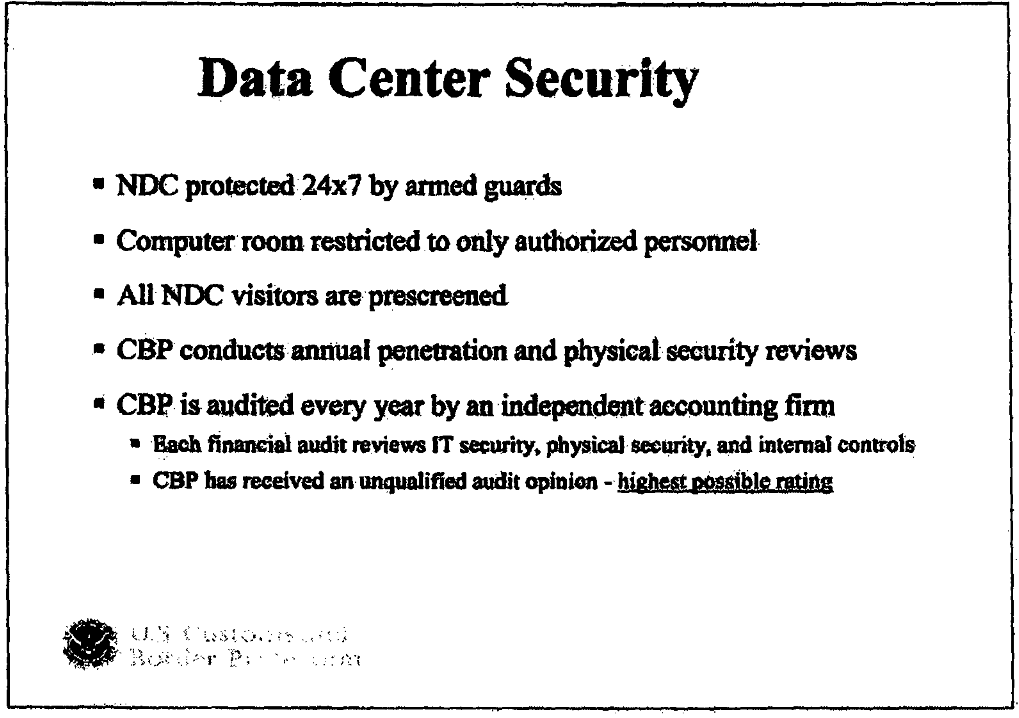
Trade Secret:

Trading partnerships (manufacturers, brokers, shippers)

Import contents and values

Persons: Employee info, frequent traveler, frequent land border crossers

Law Enforcement – known/suspected parties of interest



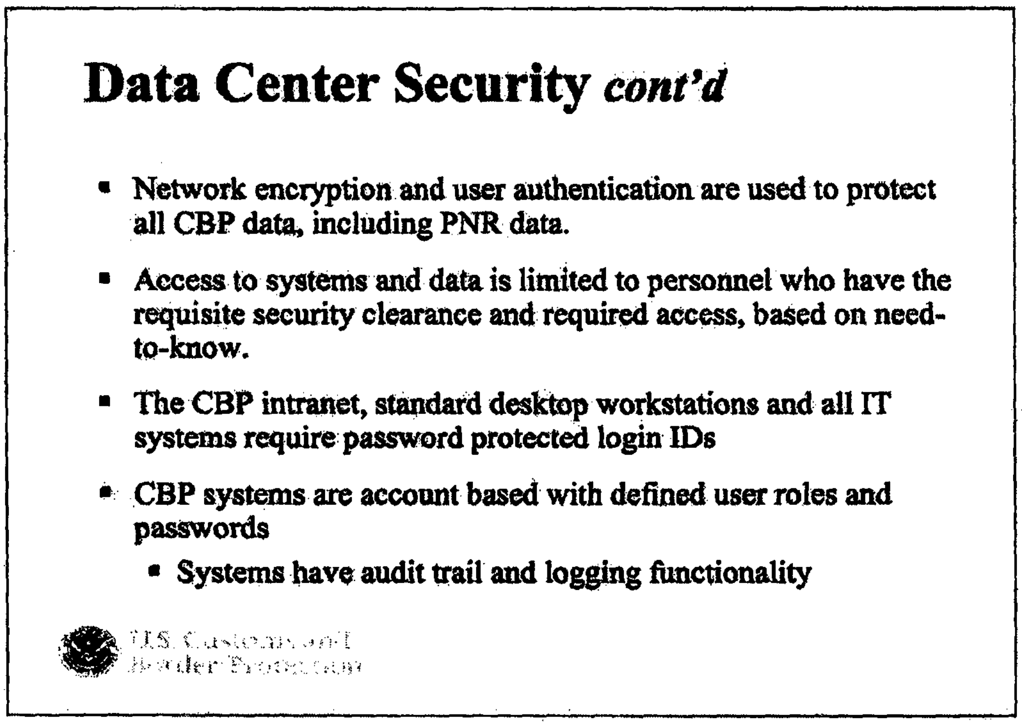
Data Center Security

- NDC protected 24x7 by armed guards
- Computer room restricted to only authorized personnel
- All NDC visitors are prescreened
- CBP conducts annual penetration and physical security reviews
- CBP is audited every year by an independent accounting firm
    - Each financial audit reviews IT security, physical security, and internal controls
    - CBP has received an unqualified audit opinion - highest possible rating

U.S. Customs and
Border Protection

The data is maintained in an extremely secure facility

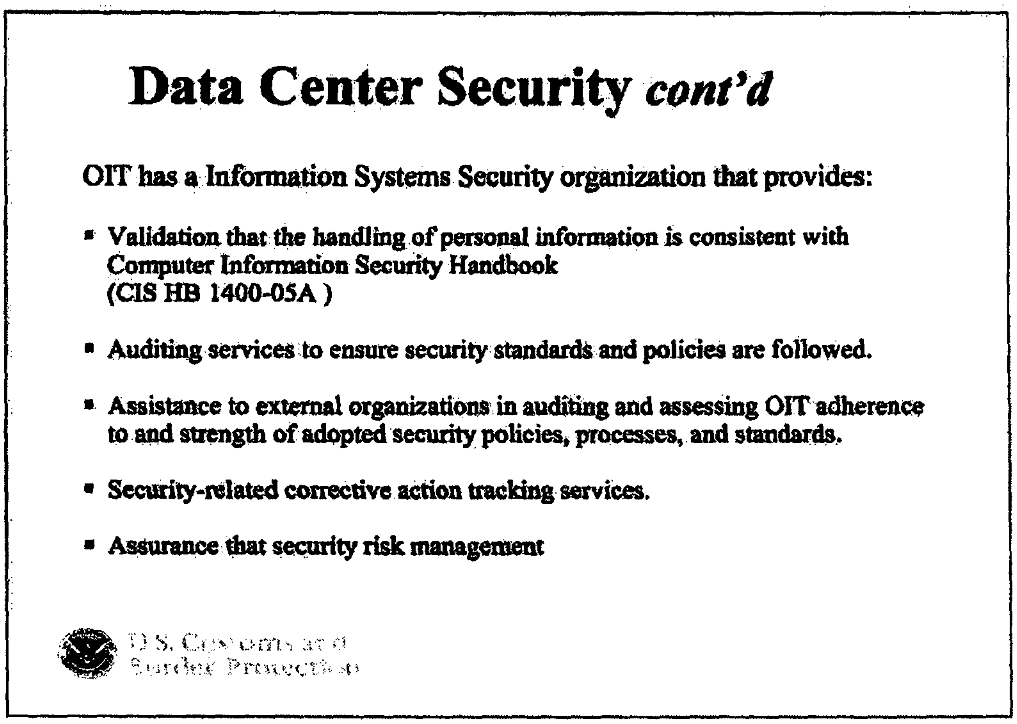
The Federal Information Security Management Act (FISMA) and the Computer Security Act require that every government organization provide computer security awareness training to all of its employees.



Data Center Security *cont'd*

- Network encryption and user authentication are used to protect all CBP data, including PNR data.
- Access to systems and data is limited to personnel who have the requisite security clearance and required access, based on need-to-know.
- The CBP intranet, standard desktop workstations and all IT systems require password protected login IDs
- CBP systems are account based with defined user roles and passwords
  - Systems have audit trail and logging functionality

U.S. Customs and
Border Protection

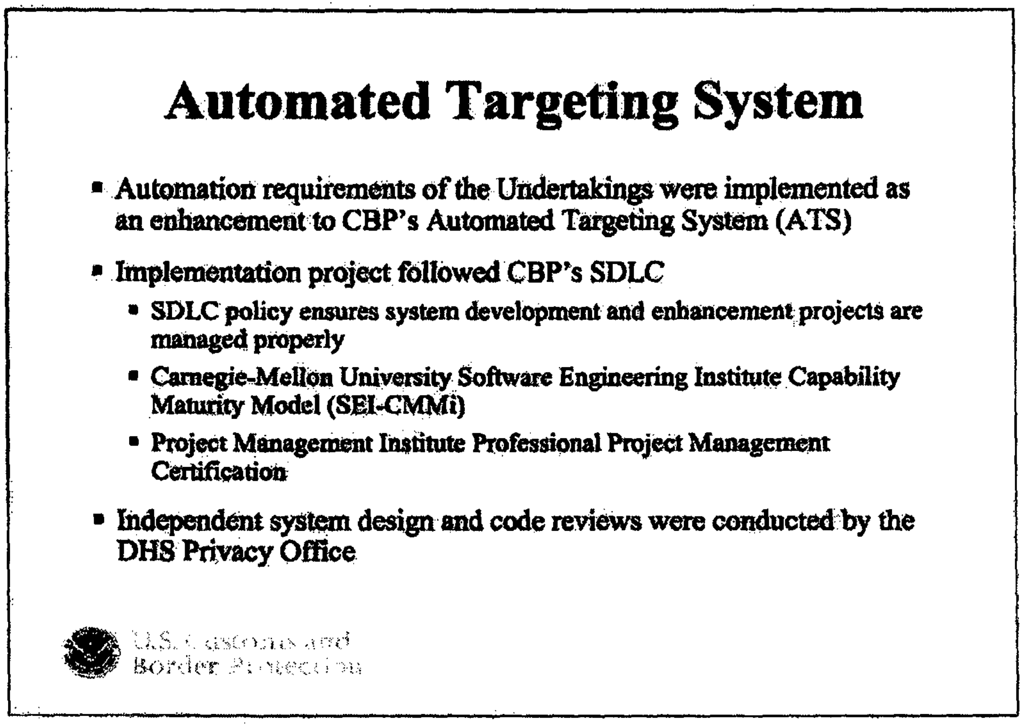


Data Center Security *cont'd*

OIT has a Information Systems Security organization that provides:

- Validation that the handling of personal information is consistent with Computer Information Security Handbook (CIS HB 1400-05A)
- Auditing services to ensure security standards and policies are followed.
- Assistance to external organizations in auditing and assessing OIT adherence to and strength of adopted security policies, processes, and standards.
- Security-related corrective action tracking services.
- Assurance that security risk management

U.S. Customs and Border Protection

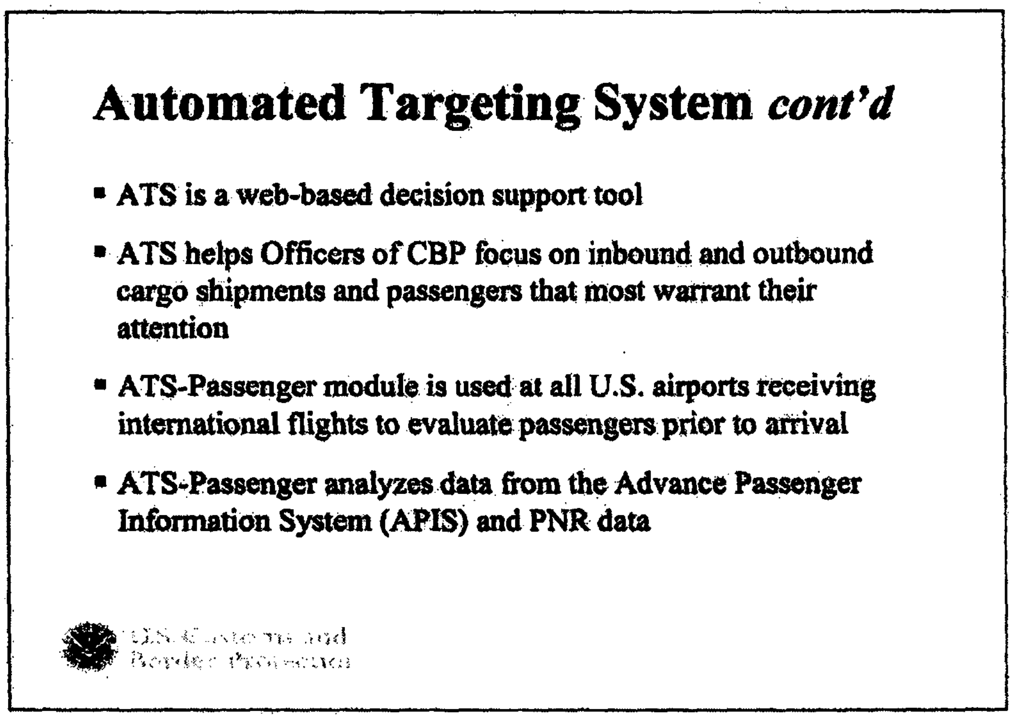


Automated Targeting System

- Automation requirements of the Undertakings were implemented as an enhancement to CBP's Automated Targeting System (ATS)
- Implementation project followed CBP's SDLC
  - SDLC policy ensures system development and enhancement projects are managed properly
  - Carnegie-Mellon University Software Engineering Institute Capability Maturity Model (SEI-CMMi)
  - Project Management Institute Professional Project Management Certification
- Independent system design and code reviews were conducted by the DHS Privacy Office

U.S. Customs and Border Protection

CBP provides Project Management training in preparation for professional certification by PMI



Automated Targeting System *cont'd*

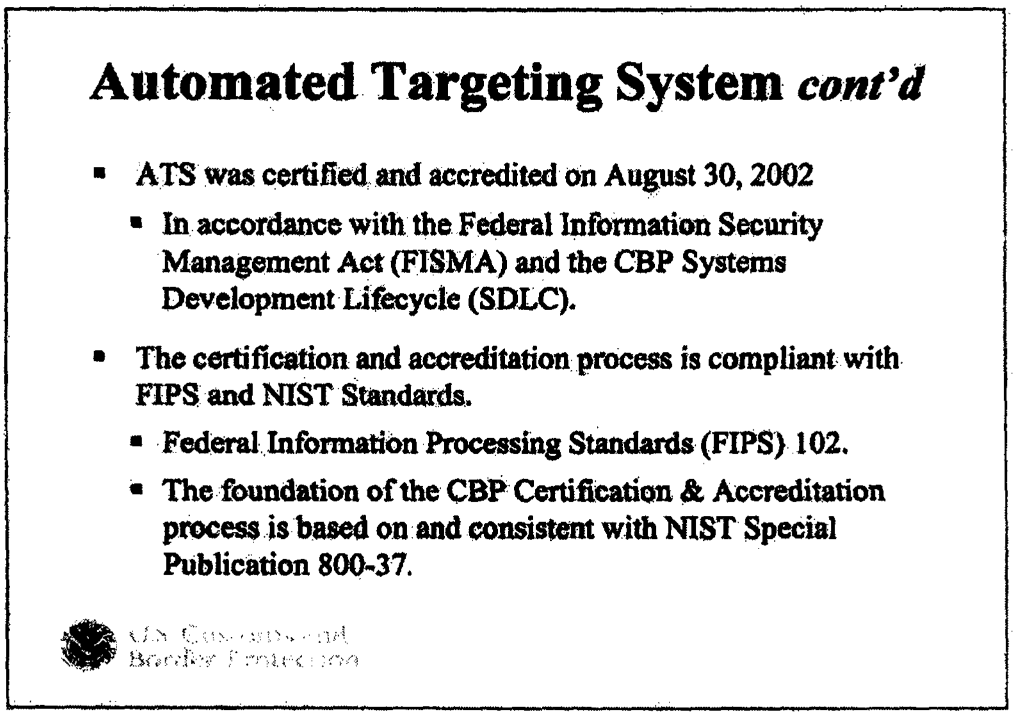
- ATS is a web-based decision support tool
- ATS helps Officers of CBP focus on inbound and outbound cargo shipments and passengers that most warrant their attention
- ATS-Passenger module is used at all U.S. airports receiving international flights to evaluate passengers prior to arrival
- ATS-Passenger analyzes data from the Advance Passenger Information System (APIS) and PNR data

U.S. Customs and Border Protection

ATS is an established program that started in the legacy Customs Service in 1992. the first Passenger processing module began in 1996

ATS-P analyzes data using algorithms to determine risk relative to other passengers to help officers focus their inspection efforts

Will see more about how data in ATS-P is used tomorrow at either the NTC or at the PAU



Automated Targeting System *cont'd*

- ATS was certified and accredited on August 30, 2002
  - In accordance with the Federal Information Security Management Act (FISMA) and the CBP Systems Development Lifecycle (SDLC).
- The certification and accreditation process is compliant with FIPS and NIST Standards.
  - Federal Information Processing Standards (FIPS) 102.
  - The foundation of the CBP Certification & Accreditation process is based on and consistent with NIST Special Publication 800-37.

U.S. Customs and Border Protection

The certification and accreditation process is compliant with NIST Federal Information Processing Standards (FIPS) 102, which includes a complete assessment of all documentation and system independent validation and verification (IV&V) to ensure that the system has appropriate security controls. The foundation of the CBP Certification & Accreditation process is based on and consistent with NIST Special Publication 800-37.

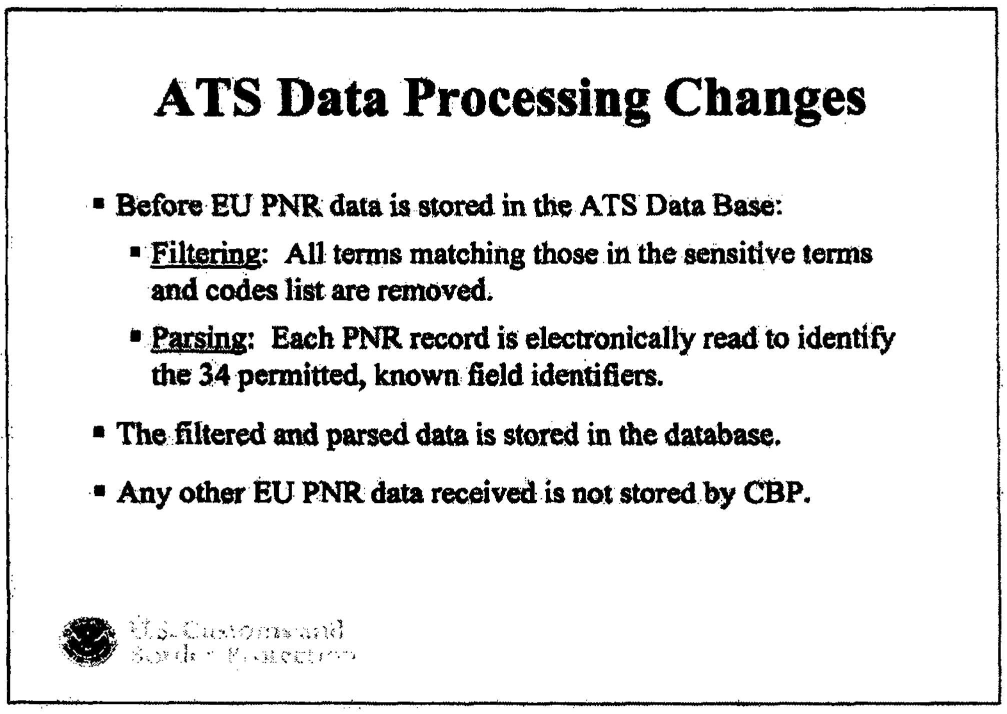
low/ High (b)(2)/(b)(7)(E)

A Valid user id and password are required for ATS

Employees are reminded of the penalties for unauthorized disclosure of information every time they log in low/High (b)(2)/(b)(7)(E)

Before requesting download of a PNR record, users must consent to using the data properly

The airport code is also checked



ATS Data Processing Changes

- Before EU PNR data is stored in the ATS Data Base:
  - Filtering: All terms matching those in the sensitive terms and codes list are removed.
  - Parsing: Each PNR record is electronically read to identify the 34 permitted, known field identifiers.
- The filtered and parsed data is stored in the database.
- Any other EU PNR data received is not stored by CBP.

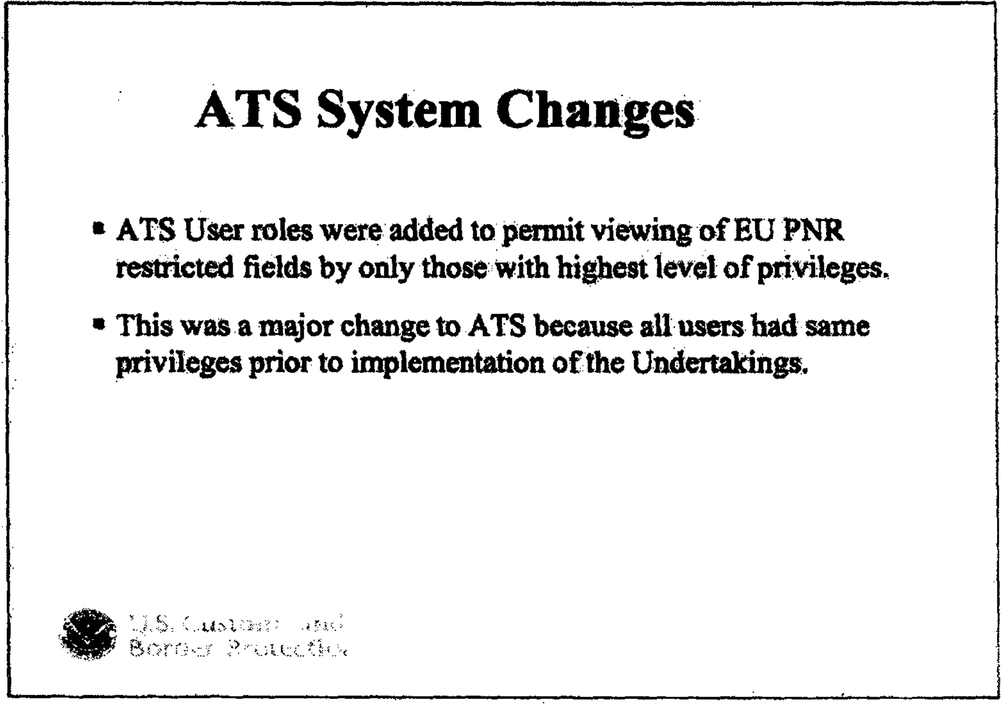
U.S. Customs and
Border Protection

Once the sensitive word list was agreed upon, the filtering code was straightforward and implemented early

Implementation of the parsing was the most time-consuming change to implement. The changes were complex because each airline creates PNR data slightly differently (no agreed-upon standard exists for PNR data, unlike cargo manifests and other widely-shared information).

Known fields that cannot be stored per the undertakings are discarded (i.e. not written to the data base)

Unknown field identifiers are discarded, too.



ATS System Changes

- ATS User roles were added to permit viewing of EU PNR restricted fields by only those with highest level of privileges.
- This was a major change to ATS because all users had same privileges prior to implementation of the Undertakings.

U.S. Customs and Border Protection

Adding user roles was a major change in design

High (b)(2)/(b)(7)(E)

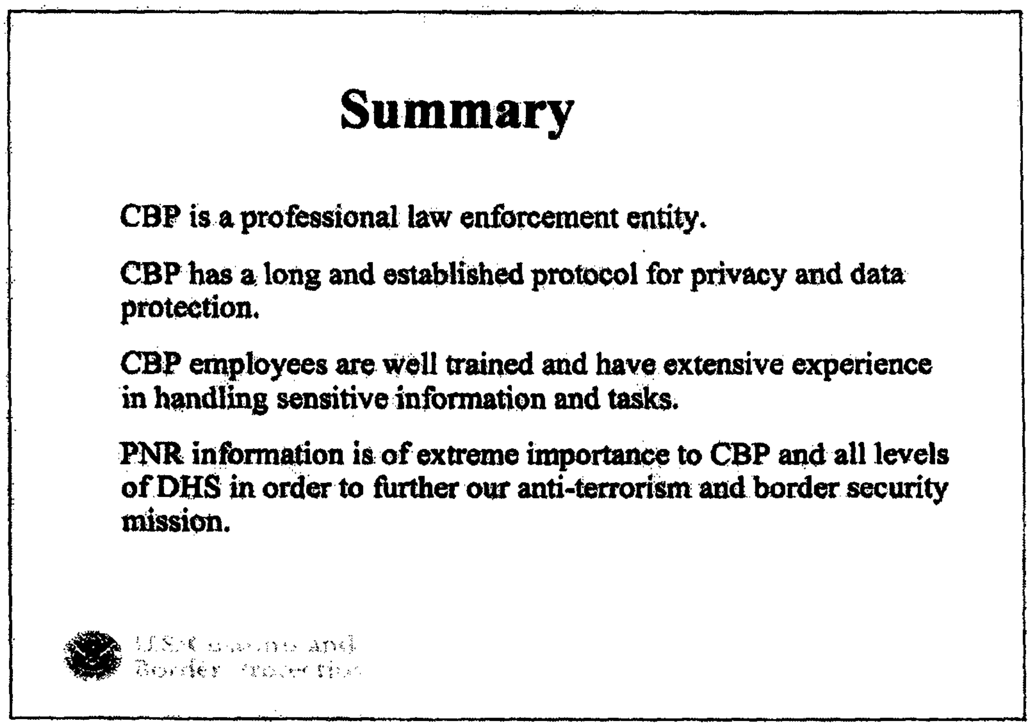
This is test data

High (b)(2)/(b)(7)(E)

High (b)(2)/(b)(7)(E)

High (b)(2)/(b)(7)(E)

High (b)(2)/(b)(7)(E)



Summary

CBP is a professional law enforcement entity.

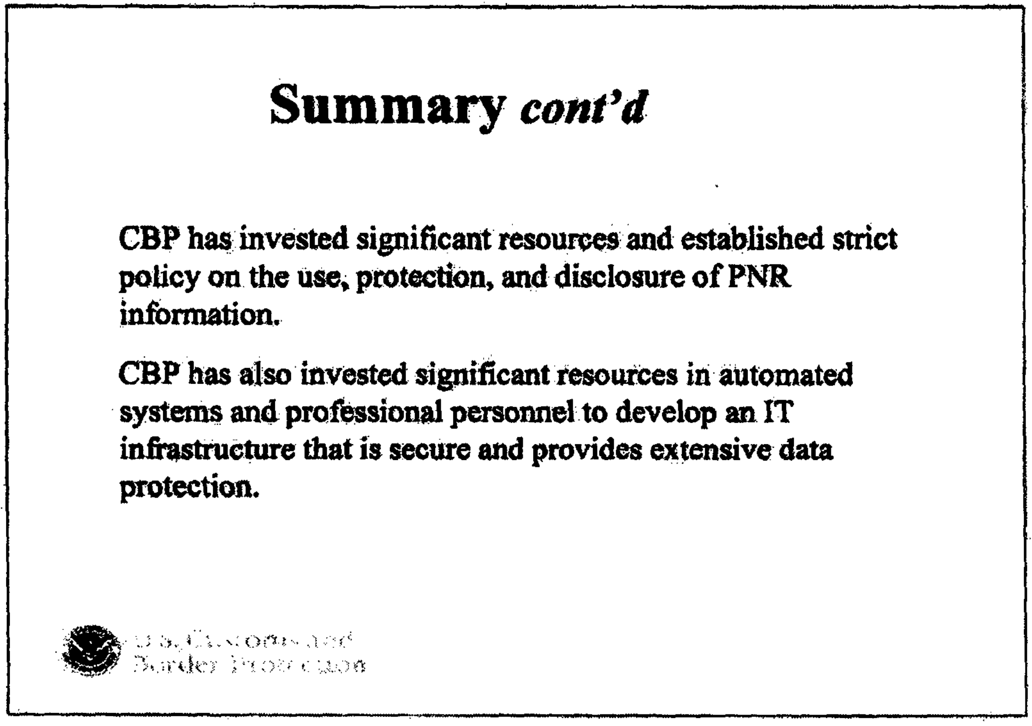
CBP has a long and established protocol for privacy and data protection.

CBP employees are well trained and have extensive experience in handling sensitive information and tasks.

PNR information is of extreme importance to CBP and all levels of DHS in order to further our anti-terrorism and border security mission.

U.S. Customs and Border Protection

Thank you for this opportunity to discuss CBP efforts to address our commitments to the PNR agreement.



Summary *cont'd*

CBP has invested significant resources and established strict policy on the use, protection, and disclosure of PNR information.

CBP has also invested significant resources in automated systems and professional personnel to develop an IT infrastructure that is secure and provides extensive data protection.

U.S. Customs and
Border Protection

U.S. Customs and Border Protection

ATS-P Working Group

Automated Targeting System – Passenger (ATS-P)

ATS-P: What it is

- Risk-assessment tool to help CBP Officers at primary decide need for additional scrutiny;
  - Screens all passengers on U.S. bound flights using data from APIS, PNR, VISA database, I-94, Personal Search Records, TECS and previous secondary inspection results;

ATS-P: Recent Events

- 11/2/2006: CBP published the System of Records Notice (SORN) regarding ATS in the Federal Register
- Media Attention:
  - 11/3/2006: The Washington Post published an article saying CBP plans to cross-check travelers' personal data with watchlists
  - 11/30/2006: Associated Press published an article saying CBP was assigning risk-scores to travelers, travelers are not allowed to see or challenge these scores, and the government would retain these scores and the accompanying PNR data for 40 years.
- Congressional Attention:
  - House and Senate interests have called for hearings
  - Chairman Bennie Thompson's staff has visited the NTC regarding ATS-P
  - Senator Joseph Lieberman and Senator Patrick Leahy, among others, have voiced concern.

ATS-P: Major Issues

- Chairman Bennie Thompson's Letter:
  - Legal authority to collect the underlying data
  - Authority and process in sharing information with third parties/Concerns over safeguarding data
  - Transparency of risk assessment process/Risk scoring
  - Issue of data retention – 40 Years
  - No ability of redress for inaccuracies
  - No clear justification for Privacy Act exemption

ATS-P: Major Issues

- System of Records Notice (SORN)
  - Access to ATS-P: Who, How?
  - Retention of PNR Data: Time and Safeguards
  - Redress process: Inherent, (b)(2)/(b)(7)(E) TRIP
  - Addressing other public comments

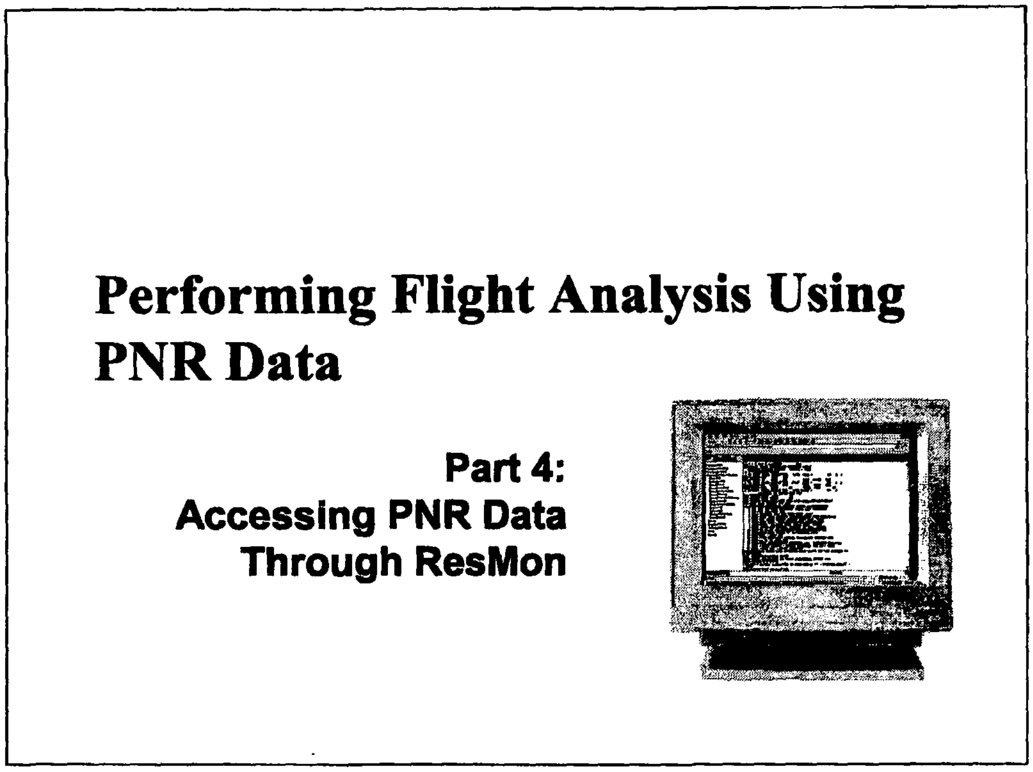
- Privacy Impact Assessment (PIA)
  - Ensure consistency with revised SORN

ATS-P: Next Steps

- ATS-P Working Group
  - Unifying a CBP message on all issues/concerns
  - Revising SORN as appropriate
  - Jointly responding to other requests
  - Recommendations on potential policy/process suggestions

U.S. DEPARTMENT OF HOMELAND SECURITY

Display the Visual



Performing Flight Analysis Using PNR Data

Part 4: Accessing PNR Data Through ResMon

Instructor Notes

Lesson Purpose: The purpose of this lesson is to present a brief introduction to the use of ResMon to display PNR data. The objectives for this lesson are shown on the next visual.

Time: 1 hour

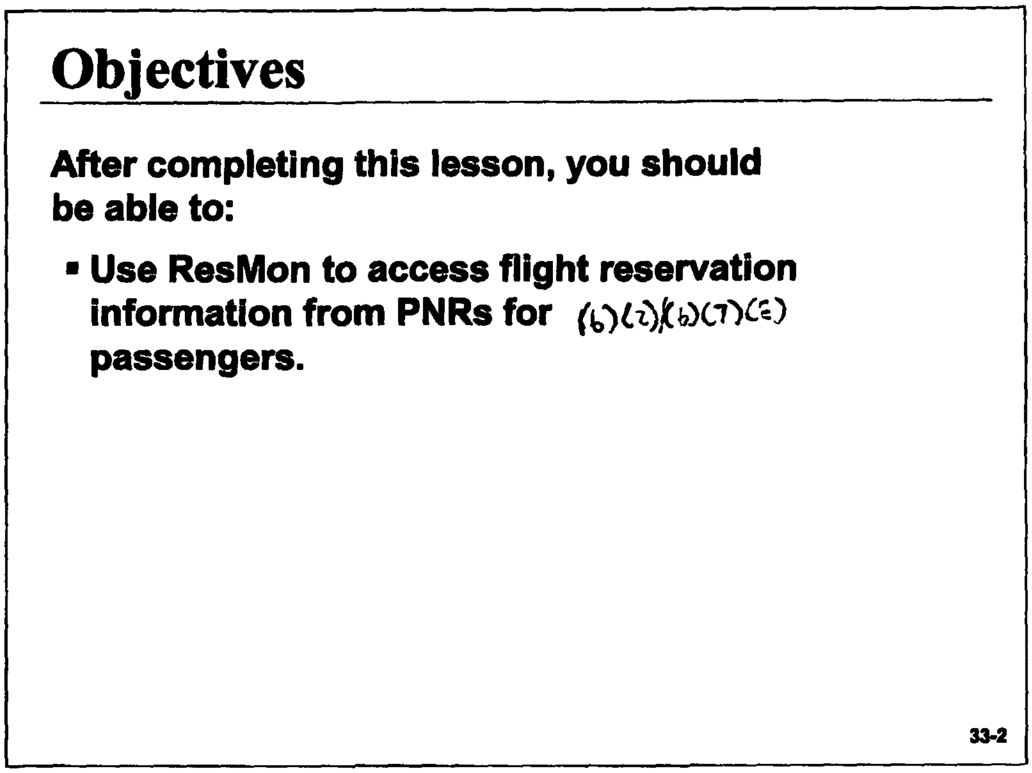
Content Outline: This presentation includes the following contents:

- Objectives
- Introduction to ResMon
  - Overview
  - Accessing ResMon
  - ResMon Tabs
  - ResMon Menu
- Displaying Flight Information
- Displaying Passenger Lists Data
- Displaying PNR Data from the Passenger List
- Displaying PNR Details
- Other ResMon Features
  - Reservation System Commands
  - Displaying All Tabs In One Window
  - Encode/Decode
  - Printing
  - Logging Out
- Exercise
- Lesson Summary

Materials:

- PowerPoint Visuals (1 through 48)
- ResMon Worksheet

Display the Visual



Objectives

After completing this lesson, you should be able to:

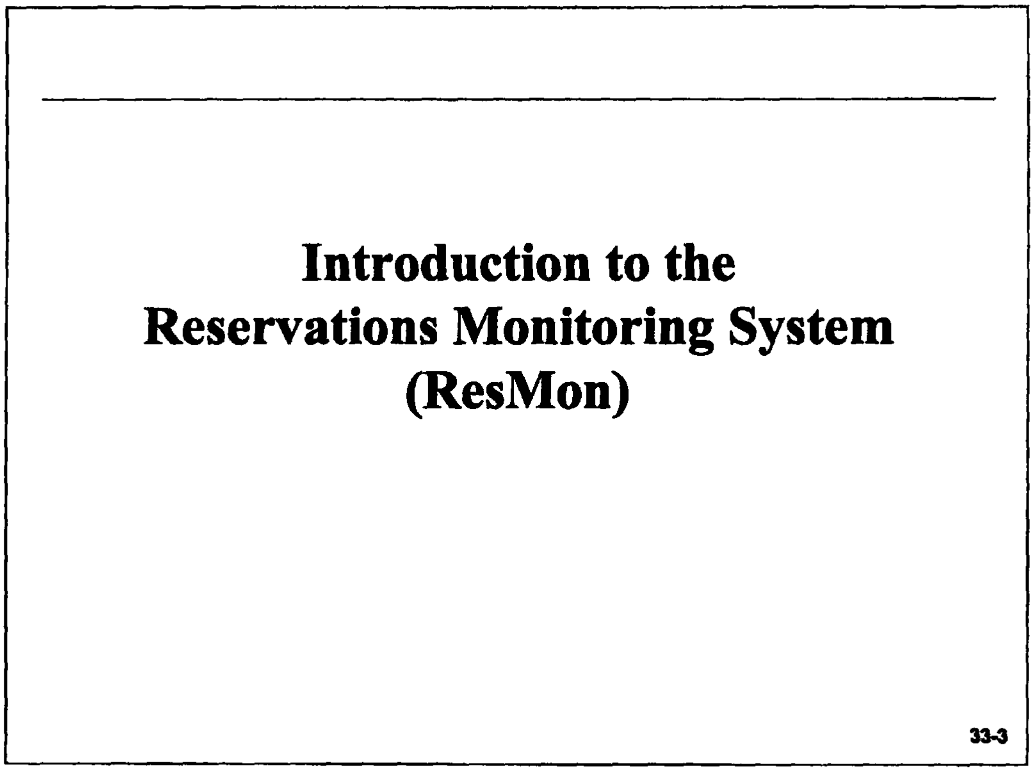
- **Use ResMon to access flight reservation information from PNRs for** (b)(2),(b)(7)(e) **passengers.**

33-2

Instructor Notes

Review the lesson objectives as listed.

Display the Visual

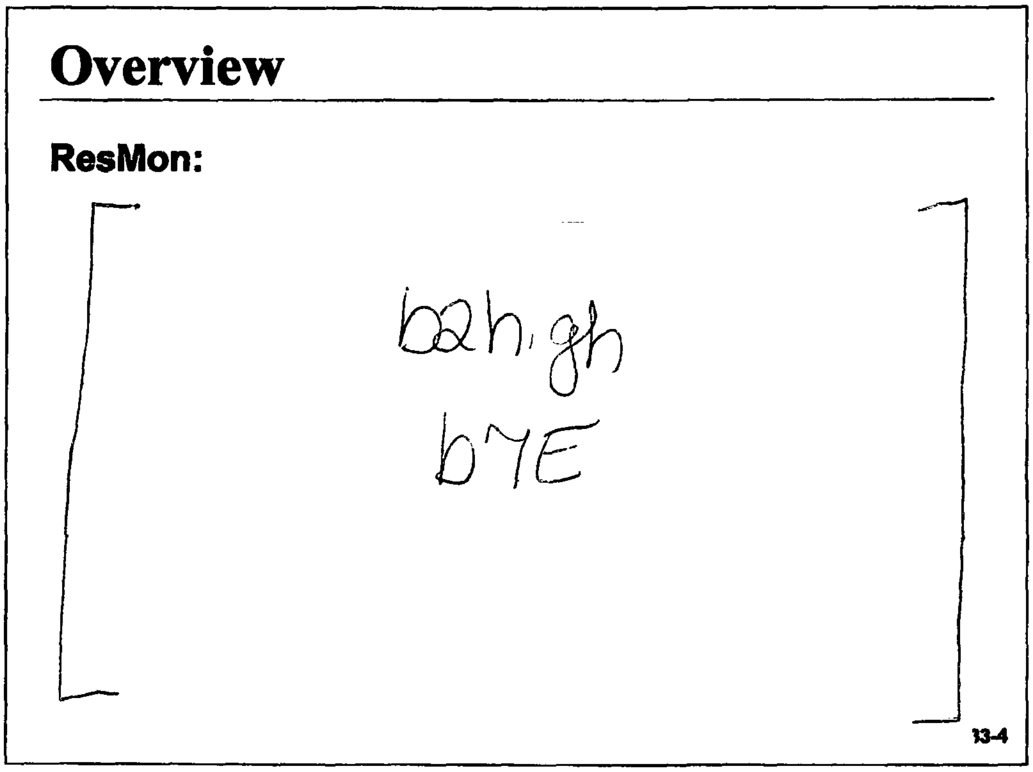


Introduction to the Reservations Monitoring System (ResMon)

33-3

Instructor Notes

Display the Visual



Overview

ResMon:

b2high

b7E

13-4

Instructor Notes

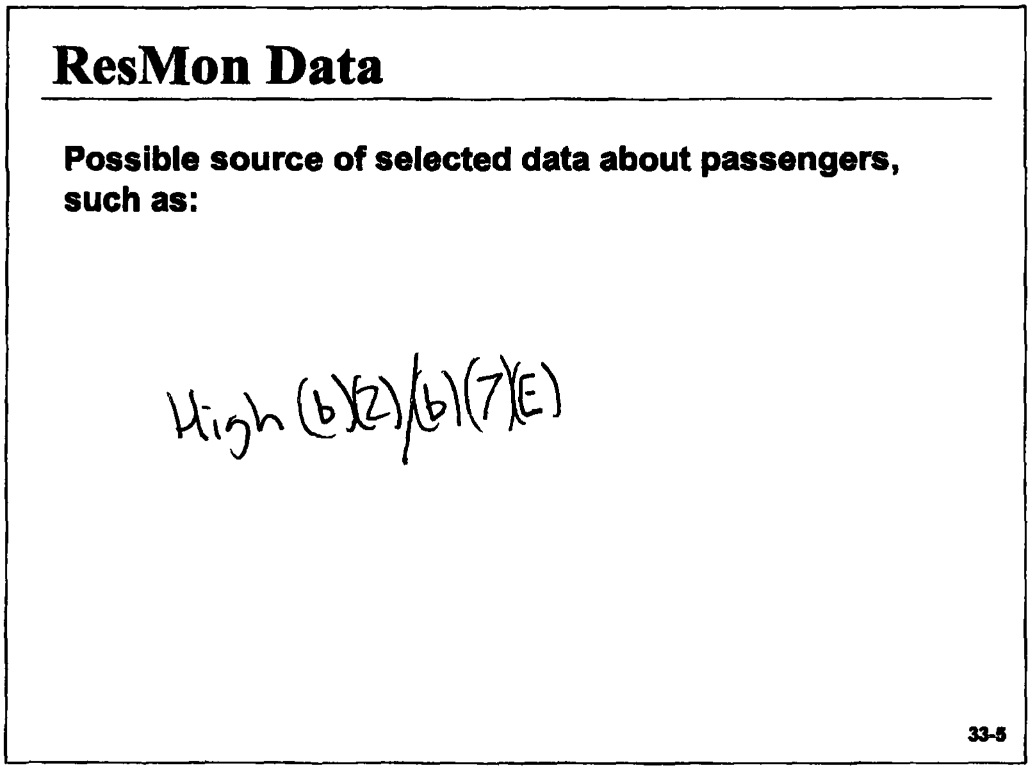
Briefly describe what ResMon is and does, as shown on the visual.

Key points:

- Supervisor and NTC approval is required for accessing European Union flights.

High (b)(2)/(b)(7)(E)

Display the Visual



ResMon Data

Possible source of selected data about passengers, such as:

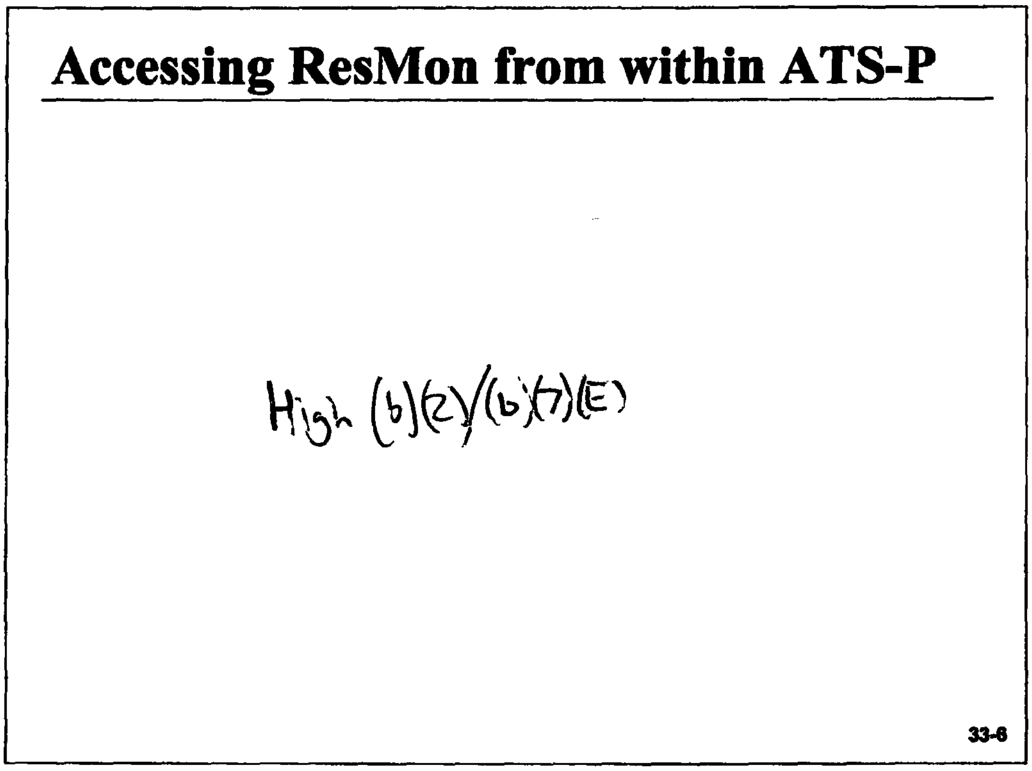
High (b)(2)/(b)(7)(E)

33-5

Instructor Notes

Briefly discuss the types of information a targeter might seek in ResMon in certain situations.

Display the Visual



Accessing ResMon from within ATS-P

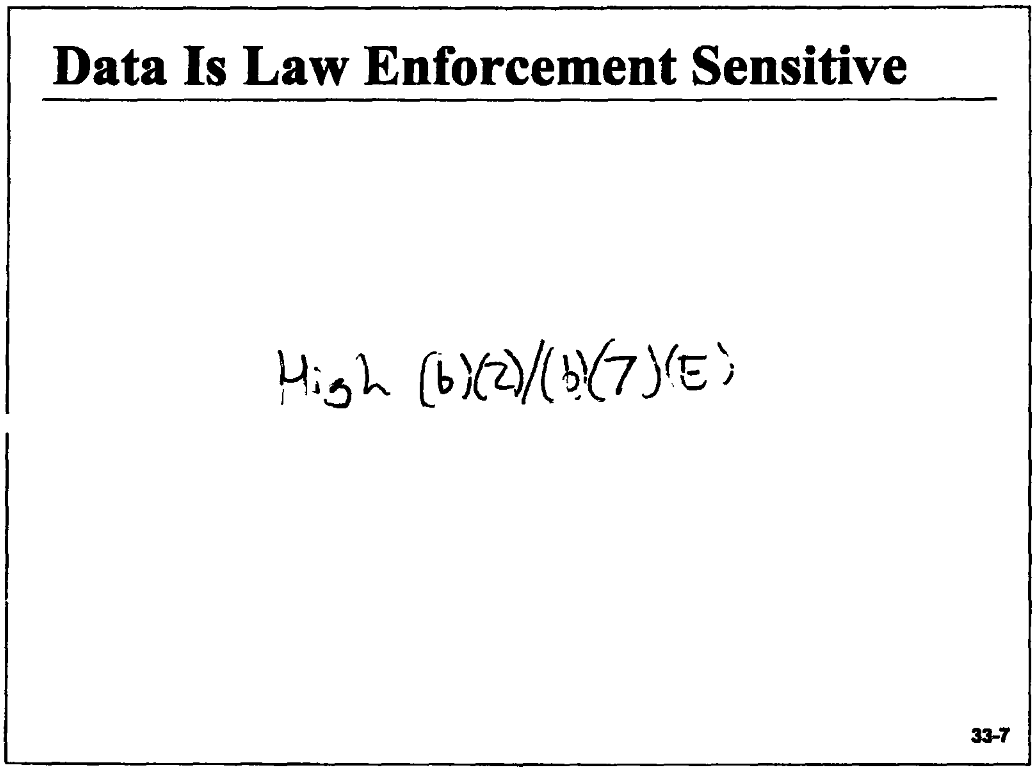
High (b)(2)/(b)(7)(E)

33-6

Instructor Notes

High (b)(2)/(b)(7)(E)

Display the Visual



Data Is Law Enforcement Sensitive

High (b)(2)/(b)(7)(E)

33-7

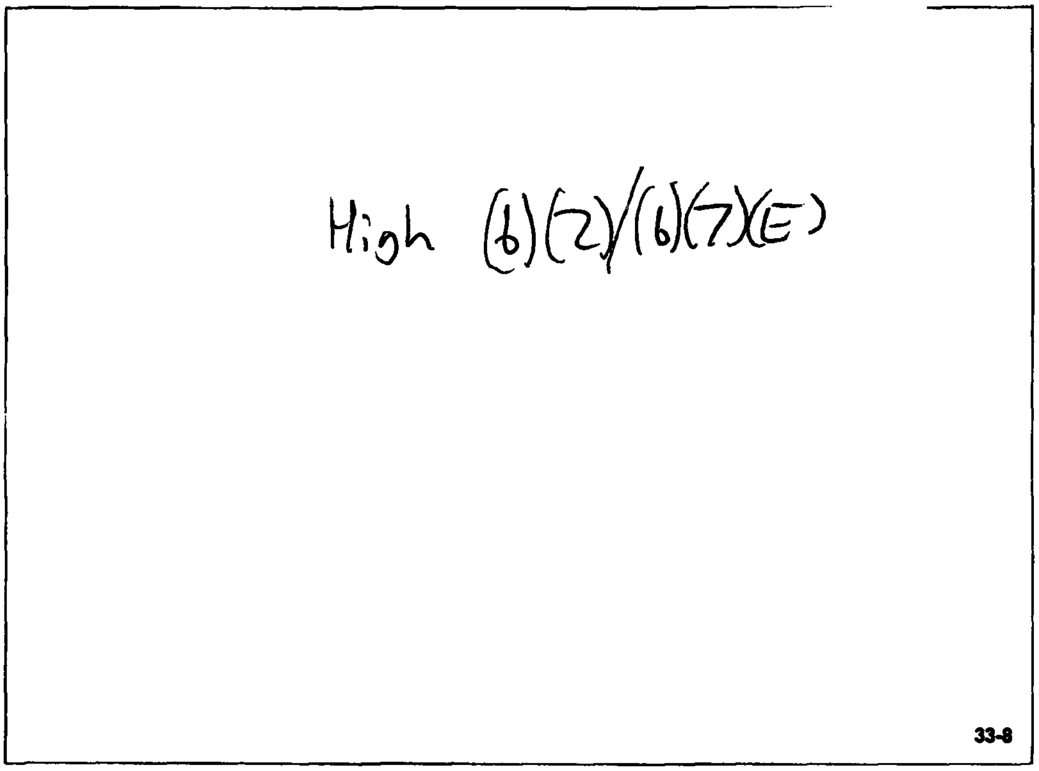
Instructor Notes

Review the warning statement shown on the visual.

Emphasize the Law Enforcement Sensitive nature of ResMon information.

High (b)(2)/(b)(7)(E)

Display the Visual



High (b)(2)/(b)(7)(E)

33-8

Instructor Notes

Explain the following points:

High (b)(2)/(b)(7)(E)

Display the Visual

High (b)(2)/(b)(7)(E)

33-9

Instructor Notes

Point out that:

- High (b)(2)/(b)(7)(E)
-
- System connection information is shown on the screen. If you have trouble and need technical help, it's good to have this information.

Display the Visual

High (b)(2)/(b)(7)(E)

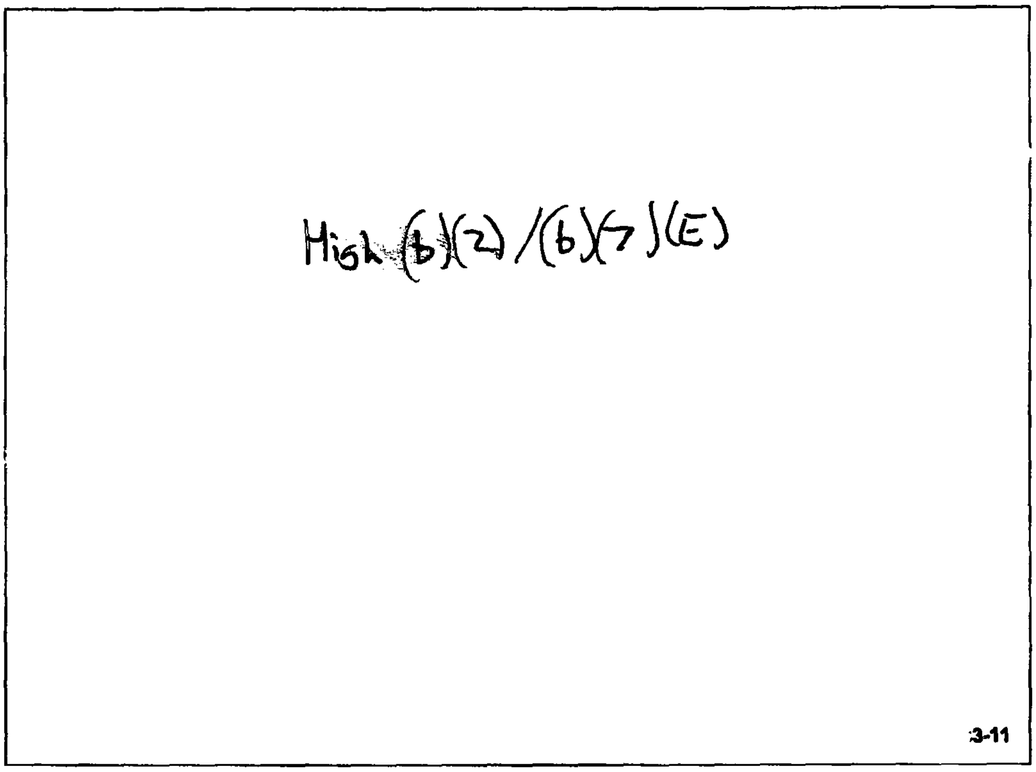
33-10

Instructor Notes

Briefly describe the five ResMon tabs.

Explain that the use of each of these tabs will be discussed in detail in this lesson.

Display the Visual



High (b)(2)/(b)(7)(E)

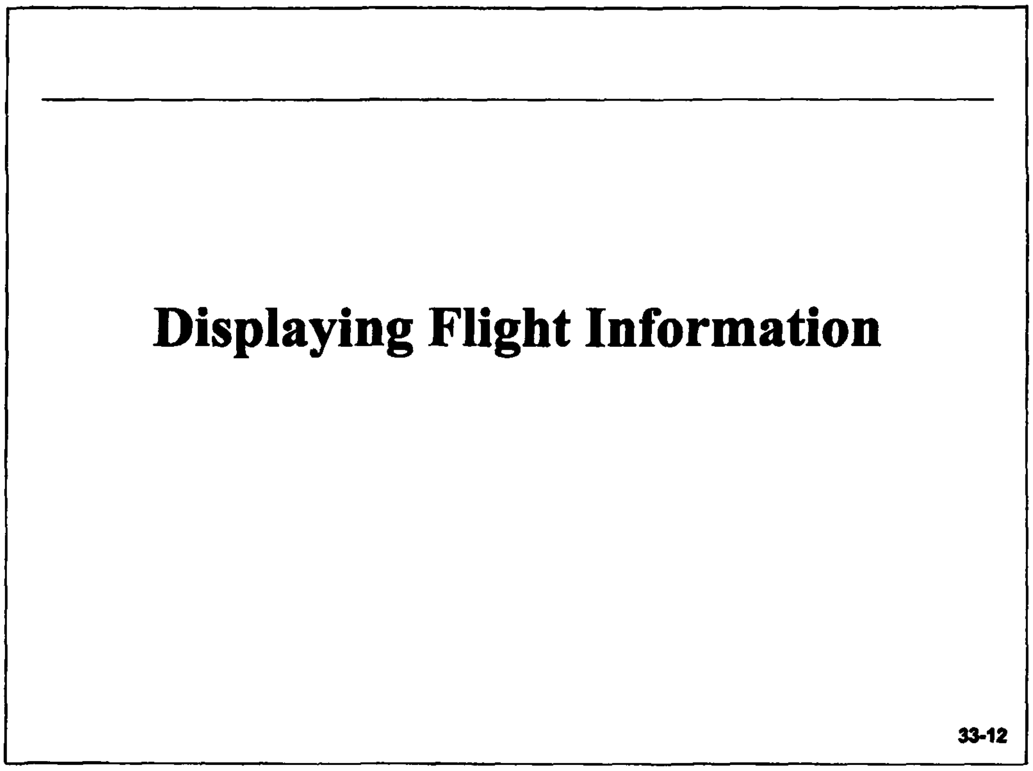
3-11

Instructor Notes

Describe the use of the ResMon menu as shown on the visual.

High (b)(2)/(b)(7)(E)

Display the Visual



Displaying Flight Information

33-12

Instructor Notes

Display the Visual

High (b)(2)/(b)(7)(E)

33-13

Instructor Notes

Walk through the steps for pulling up the flight schedule for the selected airline. **Have the class perform the steps with you.**

-
- High (b)(2)/(b)(7)(E)

Display the Visual

High (b)(2)/(b)(7)(E)

33-14

Instructor Notes

The Schedule Information box opens.

-
-

High (b)(2)/(b)(7)(E)

Display the Visual

High (b)(2)/(b)(7)(E)

33-15

Instructor Notes

The flight schedule is displayed for all flights meeting the search criteria.

Point out the:

High (b)(2)/(b)(7)(E)

Display the Visual

High (b)(2)/(b)(7)(E)

33-16

Instructor Notes

Demonstrate how to display data for a specific flight:

-
-
-

High (b)(2)/(b)(7)(E)

Display the Visual

High (b)(2)/(b)(7)(E)

33-17

Instructor Notes

Point out the types of detailed information that are displayed for the flight.

High (b)(2)/(b)(7)(E)

Display the Visual

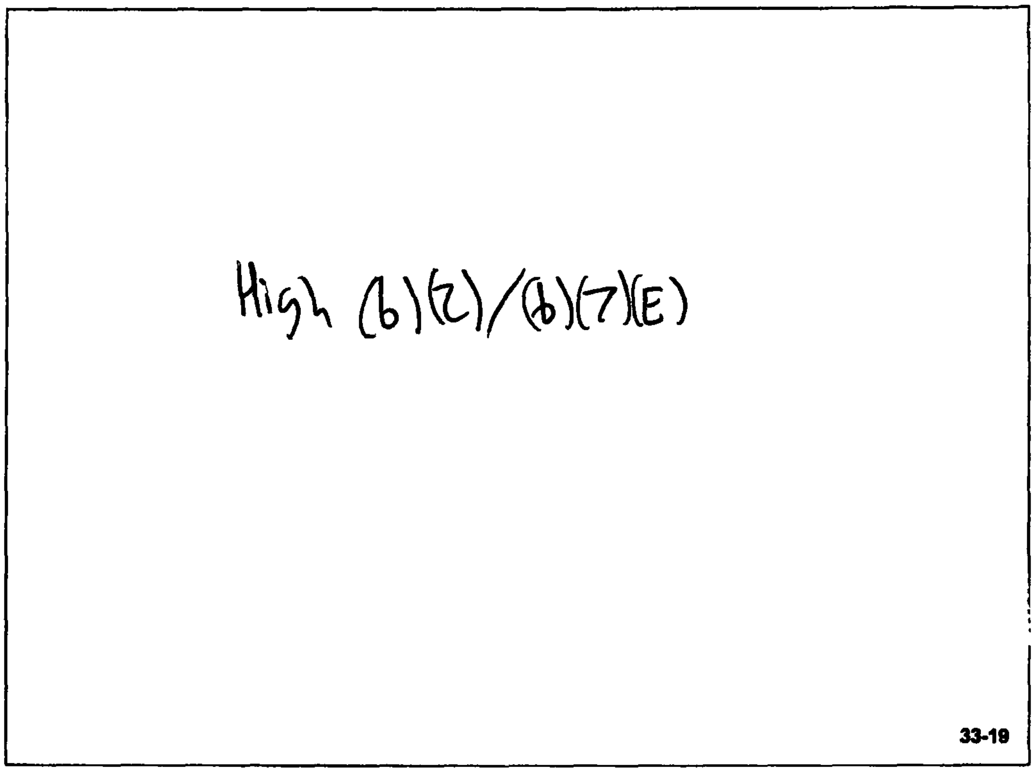
High (b)(2)/(b)(7)(E)

33-18

Instructor Notes

High (b)(2)/(b)(7)(E)

Display the Visual



High (b)(2)/(b)(7)(E)

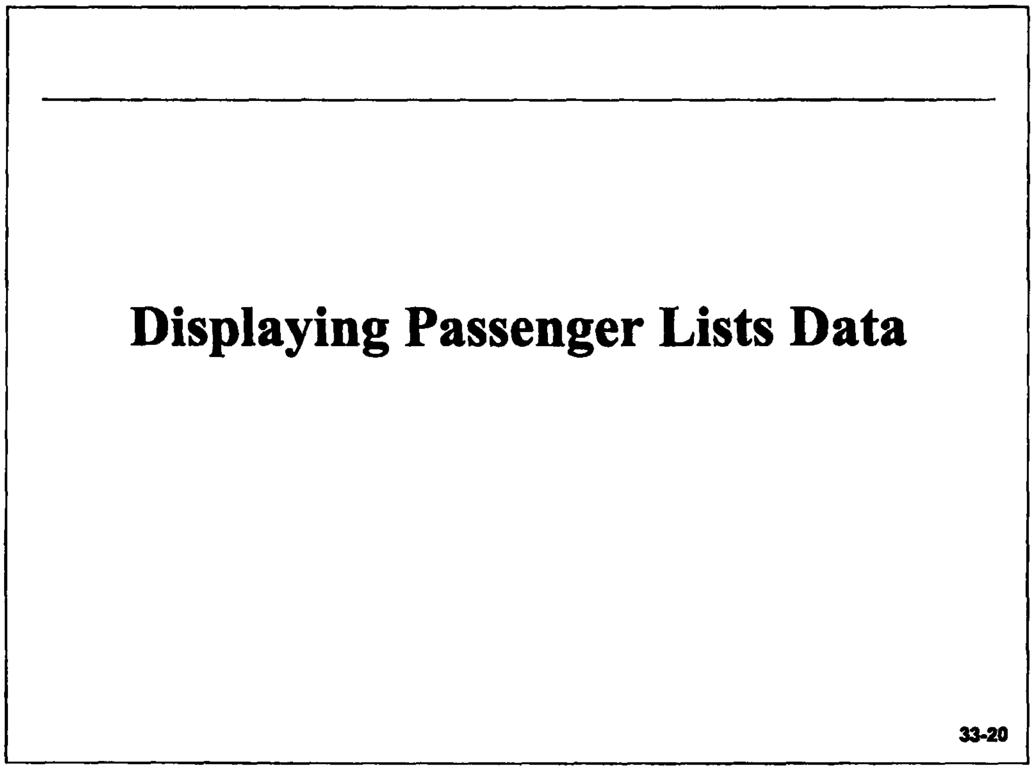
33-19

Instructor Notes

High (b)(2)/(b)(7)(E)

Describe the information displayed on this screen.

Display the Visual



Displaying Passenger Lists Data

33-20

Instructor Notes

Display the Visual

High (b)(2)/(b)(7)(E)

33-21

Instructor Notes

High (b)(2)/(b)(7)(E)

-

Display the Visual

High (b)(2)/(b)(7)(E)

Instructor Notes

High (b)(2)/(b)(7)(E)

Display the Visual

High (b)(2)(b)(7)(E)

33-23

Instructor Notes

High (b)(2)/(b)(7)(E)

Display the Visual

High (b)(2)/(b)(7)(E)

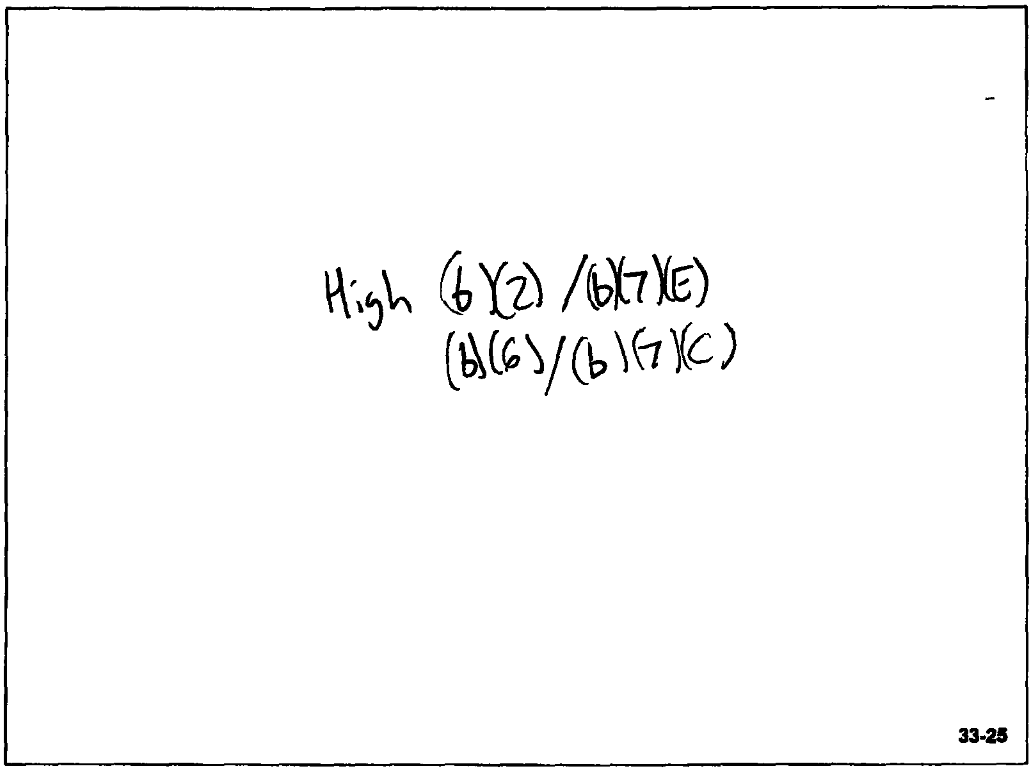
(b)(6) /(b)(7)(C)

33-24

Instructor Notes

High (b)(2) (b)(7)(E)

Display the Visual



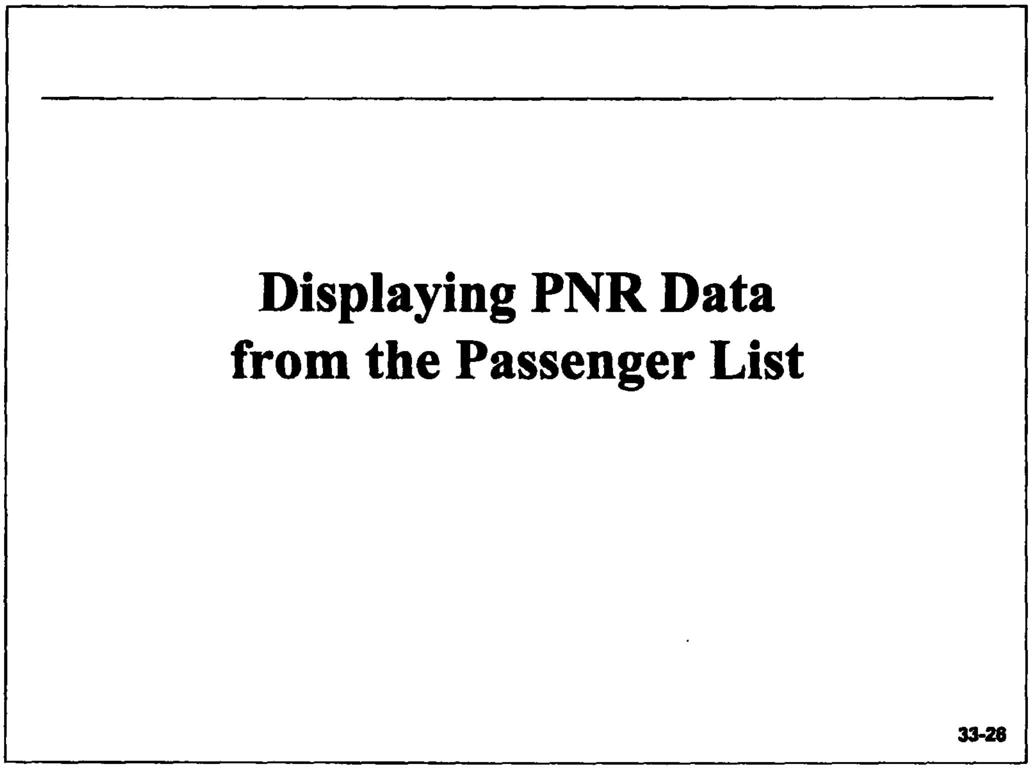
High (b)(2)/(b)(7)(E)
(b)(6)/(b)(7)(C)

33-25

Instructor Notes

High (b)(2)/(b)(7)(E)

Display the Visual



Displaying PNR Data from the Passenger List

33-28

Instructor Notes

Display the Visual

High (b)(2)/(b)(7)(E)
(b)(6)/(b)(7)(C)

33-27

Instructor Notes

- High (b)(2)/(b)(7)(E)

Display the Visual

High (b)(2)/(b)(7)(E)
(b)(6)/(b)(7)(C)

33-28

Instructor Notes

This is the window with all PNRs displayed.

High (b)(2) (b)(7)(E)

Display the Visual

High (b)(2)(b)(7)(E)

33-29

Instructor Notes

Point out the tools for scrolling, as shown.

Display the Visual

High (b)(2) (b)(7)(E)
(b)(6) (b)(7)(C)

33-30

Instructor Notes

High (b)(2)/(b)(7)(E)

Display the Visual

High (b)(2)/(b)(7)(E)

33-31

Instructor Notes

High (b)(2)/(b)(7)(E)

Display the Visual

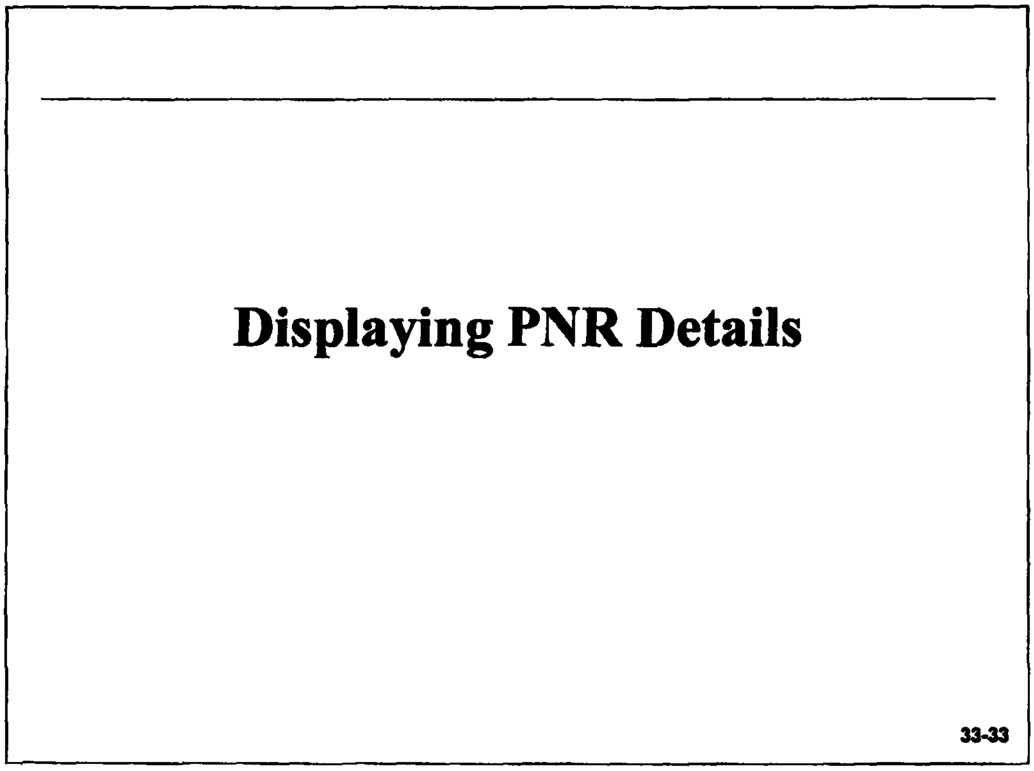
High (b)(2)/(b)(7)(E)

33-32

Instructor Notes

Briefly review the data that is displayed.

Display the Visual

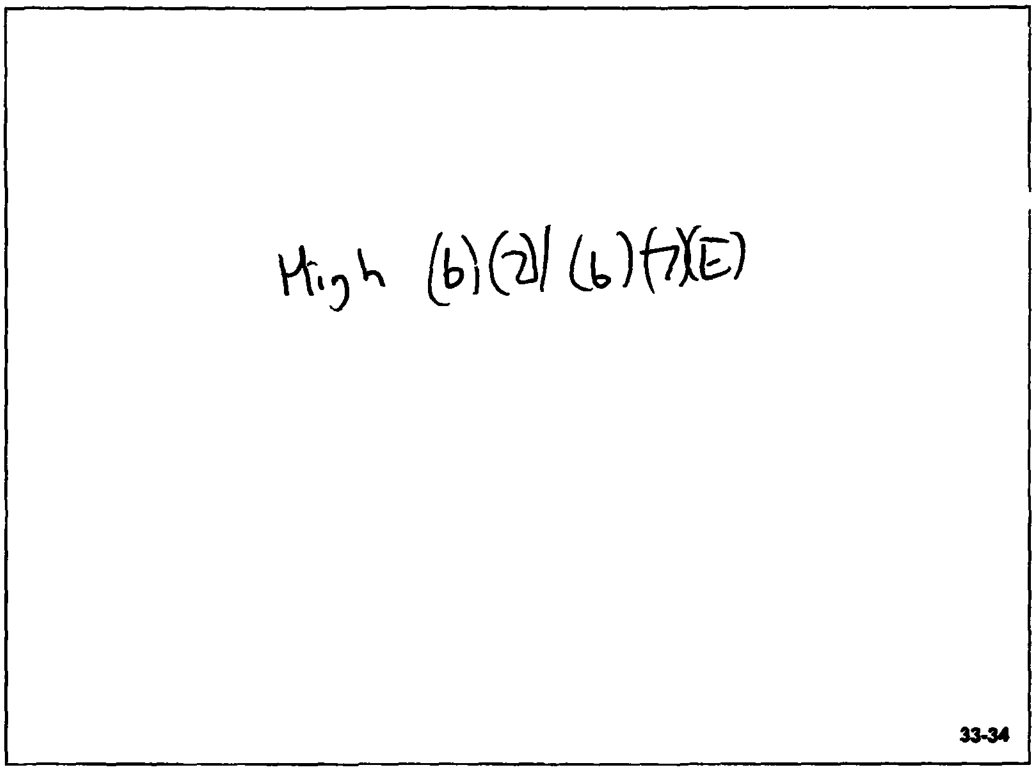


Displaying PNR Details

33-33

Instructor Notes

Display the Visual



High (b)(2)/(b)(7)(E)

33-34

Instructor Notes

Demonstrate how to view PNR details:

High (b)(2)/(b)(7)(E)

Display the Visual

High (b)(2)/(b)(7)(E)

33-35

Instructor Notes

Demonstrate how to view the history:

High (b)(2)/(b)(7)(E)

Display the Visual

High (b)(2)/(b)(7)(E)

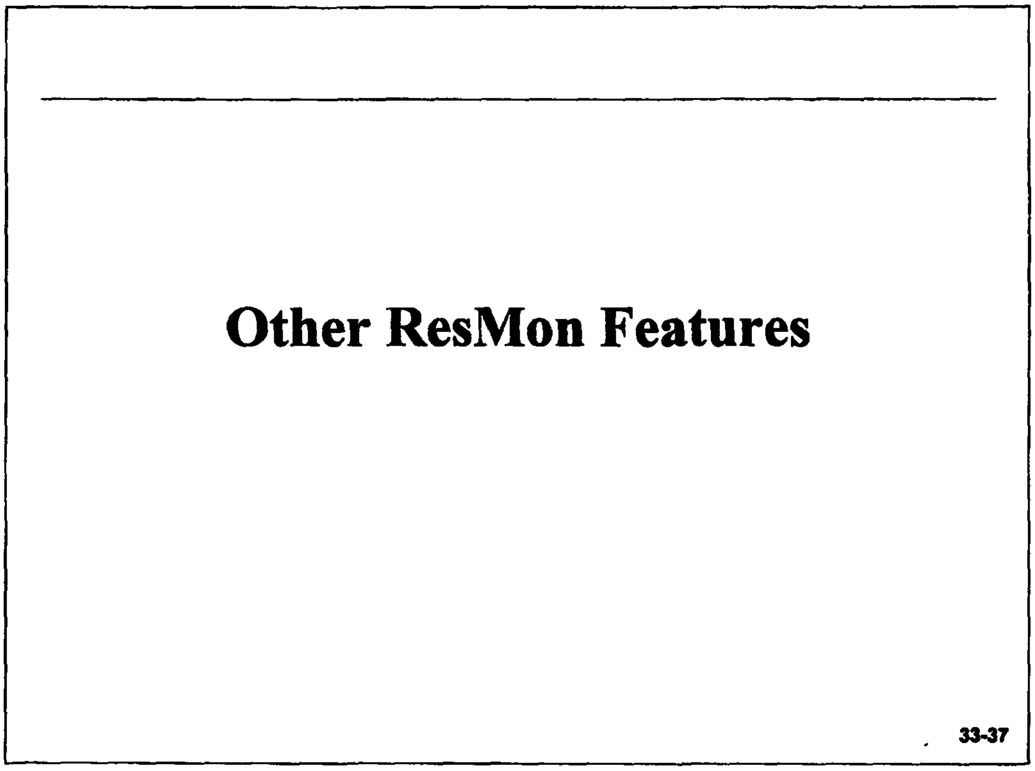
33-36

Instructor Notes

The PNR history is displayed. Point out that the Detail Info tab is active.

Review the contents of the PNR history displayed on the visual.

Display the Visual



Other ResMon Features

33-37

Instructor Notes

Display the Visual

High (b)(2)/(b)(7)(E)

33-38

Instructor Notes

High (b)(2) (b)(7)(E)

Display the Visual

High (b)(2)/(b)(7)(E)

33-39

Instructor Notes

High (b)(2)/(b)(7)(E)

Display the Visual

High (b)(2)/(b)(7)(E)

33-40

Instructor Notes

High (b)(2)/(b)(7)(E)

Display the Visual

High (b)(2)/(b)(7)(E)

33-41

Instructor Notes

This screen shows all tabs displayed on the screen.

High (b)(2)/(b)(7)(E)

Display the Visual

High (b)(2)/(b)(7)(E)

33-42

Instructor Notes

High (b)(2)/(b)(7)(E)

Demonstrate how to use this function:

High (b)(2)/(b)(7)(E)

Display the Visual

High (b)(2)/(b)(7)(E)

33-43

Instructor Notes

High (b)(2)/(b)(7)(E)

Review the displayed information.

Display the Visual

High (b)(2)/(b)(7)(E)

33-44

Instructor Notes

High (b)(2)/(b)(7)(E)

Review the displayed information.

Display the Visual

High (b)(2) / (b)(7)(E)
(b)(6) / (b)(7)(C)

33-45

Instructor Notes

High (b)(2)/(b)(7)(E)

Display the Visual

High (b)(2) (b)(7)(E)

33-46

Instructor Notes

High (b)(2)/(b)(7)(E)

Display the Visual

High (b)(2)(b)(7)(E)

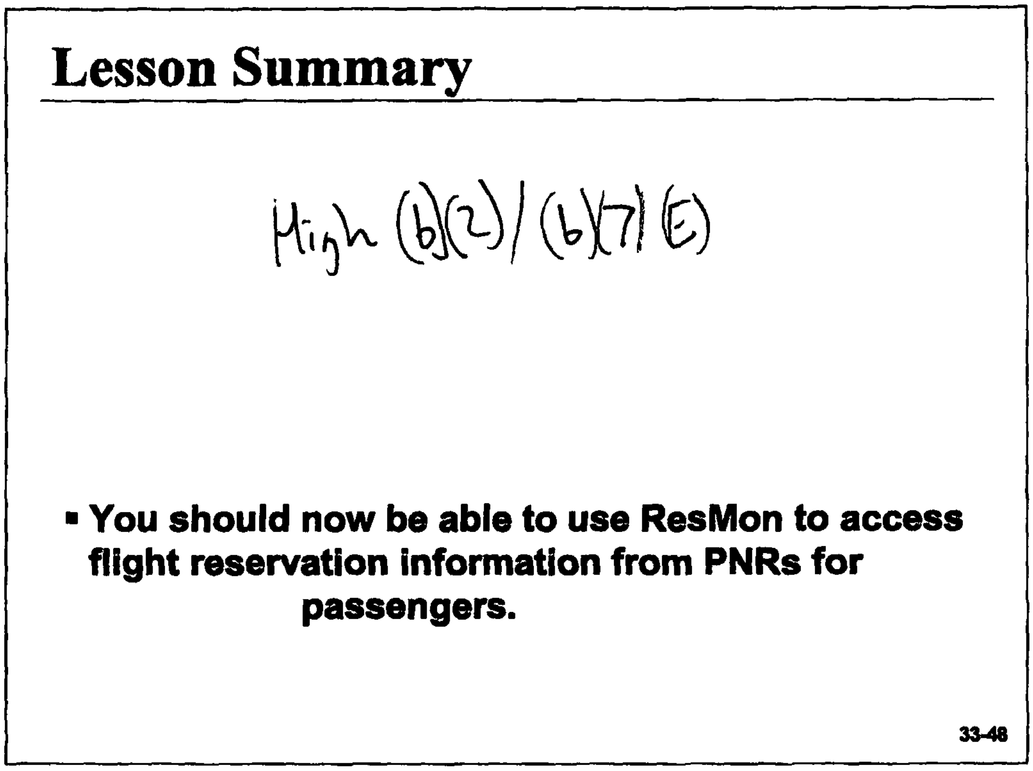
33-47

Instructor Notes

Complete the exercise as follows:

1. Ask the participants to record their answers on Worksheet 45, ResMon Worksheet.
2. Review the exercise instructions, as shown.
3. Give them 15 minutes to conduct their research. Then ask volunteers to share what they found.

Display the Visual



Lesson Summary

High (b)(2)/(b)(7)(E)

- You should now be able to use ResMon to access flight reservation information from PNRs for passengers.

33-48

Instructor Notes

Summarize the lesson, as shown.

Ask if there are any questions about the content of this lesson.

Tell the class that the next lesson will cover creating ad hoc queries in ATS-P to access PNRs.