Privacy Impact Assessment
for

CBP License Plate Reader Technology

DHS/CBP/PIA-049

December 11, 2017

Contact Point
Antonio Trindade
Associate Chief, U.S. Border Patrol
U.S. Customs and Border Protection
(202) 325-4601

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) uses a combination of surveillance systems, including license plate reader technology, to provide comprehensive situational awareness along the United States border to assist CBP in detecting, identifying, apprehending, and removing individuals illegally entering the United States at and between ports of entry or otherwise violating U.S. law. License plate reader technology includes commercially available technologies such as fixed and mobile license plate readers. CBP is conducting this Privacy Impact Assessment (PIA) to provide public notice of this CBP-owned and operated technology, assess the privacy risks, and describe the steps CBP is taking to mitigate them.

Introduction

CBP is responsible for securing the borders of the United States while facilitating lawful international trade and travel. CBP employs various technologies to enforce hundreds of U.S. laws and regulations at the border, including immigration and narcotics enforcement laws. To meet these vast mission requirements CBP relies on a variety of law enforcement tools and techniques for law enforcement and border security. One such tool is the collection, use, and retention of data collected using license plate reader technology. License plate reader (LPR) technology generally consists of a high-speed camera or cameras, and related equipment, mounted on vehicles or in fixed locations that automatically and without direct human control locate, focus on, and photograph license plates and vehicles that come into range of the device. The system then automatically converts the digital photographic images of license plates and associated data into a computer-readable format. This computer-readable format (also referred to here as a “read”) may contain the following information: (1) license plate number; (2) digital image of the license plate as well as the vehicle’s make and model; (3) state or province of registration; (4) camera identification (*i.e.*, camera owner and type); (5) Global Positioning System (GPS) coordinates[1] of the image capture, or other location information taken at the time the information was captured; and (6) date and time of observation. As with all LPR systems, CBP LPR systems may also capture (within the image) the environment surrounding a vehicle, which may include drivers and passengers. LPR technology is designed to collect information from all vehicles that pass the camera.

This PIA describes and assesses the privacy risks surrounding CBP’s collection and use license plate reader technology. It does not include CBP’s use of a commercial vendor’s nationwide database of license plate images and vehicle locations because CBP is not currently

[1] GPS is a satellite-based navigation system that provides location and time information anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites.

subscribing to such commercial sources. Should CBP pursue access to a commercial license plate database, CBP will either update this PIA or conduct a separate PIA to provide additional notice to the public and assess the unique privacy risks associated with the use of a commercial vendor license plate database.

Automated License Plate Readers at Primary Inspection Locations

As part of the standard land border inspection process, vehicles are presented to CBP at the vehicle primary border crossing lanes upon arrival at a land Port of Entry (POE) or Border Patrol Checkpoint.[2] At vehicle primary,[3] the CBP Officer or Agent obtains information directly from the driver and traveler(s) within the vehicle via their travel documents (*e.g.*, passport) and verbal communication. Vehicle border crossing lanes may also contain CBP-owned and operated license plate readers, which assist in querying the license plate numbers of vehicles approaching primary. Additionally, vehicle border crossing lanes may contain CBP-owned and operated radio frequency identification (RFID) readers, which will query applicable travel documents that are within the vehicle. The information collected at vehicle primary is used to query TECS[4] to assist the CBP Officer or Agent in determining the admissibility of the person(s) and otherwise inform the CBP Officer or Agent charged with enforcing other U.S. laws at the border. The CBP Officer or Agent at primary will conduct a TECS query to see if there are prior CBP violations that might indicate a need for further review as well as queries against lookouts, such as “wants and warrants,” watch list matches, etc. Additionally, the CBP Officer or Agent at primary will conduct searches of other relevant law enforcement databases based on the license plate information.[5]

As vehicles wait in lanes for the inspection process, CBP uses LPR to initiate license plate queries prior to the vehicle approaching a CBP Officer or Agent. Unlike in the air/sea travel environment in which CBP receives advanced passenger information (manifests), CBP generally does not receive information about individuals traveling to the United States by foot (pedestrian) or vehicle prior to their arrival at a POE. There are no manifests required for pedestrian travelers or private passenger vehicles entering the United States by land.[6] Because the reader is stationed

[2] A Border Patrol Checkpoint is a non-port of entry location at which vehicular immigration inspections occur. The purpose of the checkpoint is to enforce immigration law through interdiction of aliens furthering unlawful entry into or unlawfully presence in the United States, and to restrict the routes of egress from the border area thereby deterring illegal entries.

[3] The primary inspection area is the location of the initial point of contact at which a CBP Officer or Agent inspects a vehicle or conveyance and its occupants.

[4] For a thorough discussion of all law enforcement and national security checks conducted during the inspection process, as well as an assessment of privacy risk, please *see* the DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing, *available at* www.dhs.gov/privacy.

[5] CBP does not currently subscribe to a commercial vendor’s nationwide database of license plate images and vehicle locations. Should CBP pursue access to a commercial license plate database, CBP will either update this PIA or conduct a separate PIA to provide additional notice to the public and assess the unique privacy risks associated with the use of a commercial vendor license plate database.

[6] In certain instances, CBP may receive voluntary submission of passenger manifests for rail and commercial bus traffic across the U.S. border.

a short distance ahead of the primary inspection area, license plate checks may be run sooner, providing CBP with valuable extra time in the event that a particular vehicle or traveler poses a threat as verified by the law enforcement or national security checks. These readers are currently deployed for inbound and outbound traffic at ports of entry, and at Border Patrol Checkpoints.

When a vehicle enters the primary inspection lane, either at the port of entry or at a Border Patrol Checkpoint, a sensor grid determines that a vehicle has entered the lane. The sensors deploy a flash strobe that illuminates the area and the LPR cameras take a picture of the front and rear of the vehicle. The image processor unit searches the image to locate the license plate and then determines not only the license plate number, but also the state or province that issued the license plate. The image processor unit then forms the query and passes this information to the Border Patrol Client (BPC) application. The BPC is a license plate reader interface querying application used to query license plate data and information derived from documents scanned in a peripheral reader against multiple law enforcement databases. This ability enhances officer safety by providing the vehicle's registered-owner information and any associated alerts prior to entering the primary inspection area. The BPC, connected with the LPR, forms the core technology components to provide border-centric, real-time border intelligence by creating crossing records when vehicle/document information is entered into the system. This makes it possible for crossing histories to be queried in both the Land Border Web Reporting System (LBWRS) and the Automated Targeting System-Land (ATS-L) for intelligence or historical reference.

The CBP Officer or Agent sees the query results using either the BPC (at Border Patrol Checkpoints) or the Vehicle Primary Client (VPC) (at ports of entry), two different TECS modules used for primary vehicle inspections. While each land border crossing has different physical features and requirements, each automated LPR at primary consists of the following functions:

- Capture of vehicle license plate image(s);
- Transmission of the license plate numbers to TECS to conduct a query against the number in that database;
- Retrieval of results of the law enforcement query;
- Count of the number of vehicles crossing into the United States by port and by time, and providing this information for management analysis and decision making;

The automated LPR at primary supports the CBP mission for conducting inspections, including "pre-primary" observations[7] on vehicles and their occupants upon entering the United States.

Automated LPR Data Sharing with the Drug Enforcement Administration (DEA)

This PIA also serves as notice that CBP is partnering with the Drug Enforcement

[7] Pre-primary observations are observations made by CBP Officers or Agents of vehicles or conveyances and their occupants as each approach or wait to enter the primary inspection area.

Administration (DEA) to leverage each other's strategically located LPR systems. The partnership will enhance CBP and DEA enforcement capabilities. Both parties will use a web service application for query-based searches of historic LPR information, and a streaming service for real-time alerts to monitor encounters with vehicles of interest.

DEA access to CBP LPR information

CBP intends to provide DEA access to CBP ALPR information (collected at Ports of Entry and Border Patrol Checkpoints) through a real-time streaming service, however the information exchange has not started. DEA, as a user of the TECS system, can currently query CBP license plate information just like any other "level 1" TECS record[8] (such as border crossing information), pursuant to the signed DEA TECS User Agreement (1997). Pursuant to the TECS User Agreement, TECS level 1 records such as LPR information from border crossings may be shared with other TECS user agencies, including DEA. To improve the current query-based process, CBP intends to provide ALPR data collected at primary inspection points to DEA through a real-time, streaming service.[9]

If implemented, the streaming service will provide DEA with raw CBP LPR data captured only at POEs, both inbound and outbound, in order to permit DEA to monitor for encounters of license plates subject to lookouts placed in the DEA Analysis and Response Tracking System (DARTS)[10] and DEA Internet Connectivity Endeavor (DICE)[11] System. LPR data delivered through the streaming service may contain the following data elements: location of collection, date and time of collection, and images which may include front plate, rear plate, and scene.

CBP will issue an update to this PIA detailing sharing arrangements with any external partners prior to disclosing any LPR information via a streaming service.

CBP access to DEA LPR information

DEA will provide CBP with query-based access to its LPR data via a web service in order to permit users of CBP's Automated Targeting System-Land (ATS-L) to search DEA LPR data for CBP's border enforcement mission. The DEA LPR system encompasses both inbound and outbound cameras, greatly enhancing CBP border-centric information. DEA LPR data delivered through the web service may contain the following data elements: license plate number and state,

[8] For additional information regarding TECS records and information sharing processes, please see DHS/CBP/PIA-021 TECS System: Platform (August 2016), *available at* www.dhs.gov/privacy.
[9] CBP will also develop a web service to permit DEA to query historic LPR information within the TECS system as part of the Border Crossing Information SORN. This PIA will be updated when that functionality is complete.
[10] CBP's understanding is that DARTS is a de-confliction system, maintained by its Office of Special Intelligence.
[11] CBP's understanding is that DICE enables any participating federal, state, local, and tribal law enforcement agency to de-conflict investigative information, such as phone numbers, email addresses, bank accounts, plane tail numbers, and license plates, to identify investigative overlaps. The system, accessible through the Internet, allows users to be notified if an overlap occurs and provides points of contact information so users can discuss the investigative links.

location/date/time of collection, and images that may include front plate, rear plate, and scene.

Mobile and Covert License Plate Readers

In addition to the automated LPRs deployed at ports of entry and Border Patrol Checkpoints, the U.S. Border Patrol (USBP) also deploys Mobile LPRs and Covert LPRs in support of its law enforcement and border security missions. The Mobile LPR and Covert LPR technologies are designed to assist U.S. Border Patrol Agents in identifying travel patterns indicative of illegal border related activities and are designed to be easily redeployed depending on mission requirements.

Mobile LPRs are overtly mounted on CBP vehicles and record license plate information from all vehicles that pass by a CBP vehicle. Mobile LPRs are connected to the computer inside an Officer or Agent’s vehicle.

Covert LPRs are fixed, unmanned readers installed at known smuggling routes and other areas of interest. Covert LPRs are not readily identifiable as LPRs and may be hidden from view entirely. Covert LPRs are designed to be used for a set period of time while CBP is conducting an investigation of an area of interest or smuggling route. Once the investigation is complete, or the illicit activity has stopped in that area, the covert cameras are removed.

Mobile and Covert LPR Encounter Storage and Management

Each license plate that a Mobile or Covert LPR records is called an “encounter.” These encounters have location, date, and timestamp identifiers. Encounters are stored locally on the LPR device only for the amount of time needed for data transmission to a standalone server.

1. Access to the camera is through a Transmission Control Protocol/Internet Protocol (TCP/IP) address, which is controlled through proprietary software. Once purchased CBP will have sole access to this information via password protection.

2. Access controls for the standalone server will be limited access by requiring users to change their password every 90 days with password complexity mirroring existing CBP systems.

3. The encounter data will be stored on the server for no more than 2 years, unless the encounter has a nexus to an active investigation.

4. Tracking of inventory and reporting of lost or stolen equipment will be recorded and tracked per standard methods used with all USBP accountable equipment.

If the behavior of the vehicle is of law enforcement interest, or if the license plate is captured at a location possibly indicating criminal behavior, the Agent will manually search previously uploaded LPR spreadsheets stored on the standalone server, and conduct another search of law enforcement databases to which he or she already has access (such as TECS) to determine if the vehicle has been previously connected to investigatory or criminal activity.

"Hot Lists" for Local License Plates of Interest

Each Sector (or Station) is responsible for developing and maintaining a local "hot list" of license plates of interest. A license plate of interest is typically related to a vehicle or person who is the subject of an active law enforcement investigation. Each Sector will maintain its own "hot list," which is typically a list of the current top ten or twenty license plates of interest. The hot list can change daily, depending on the Sector or Station enforcement priorities.

The hot list will be used in two ways: (a) storage on the device for real time matching and (b) manual query by Agents at the Station. Mobile LPRs (on Agent vehicles) are connected to the Agent's vehicle computer, and therefore can upload the hot list directly to the LPR capture device. If a vehicle on the list passes by the Mobile LPR, it will alert the Agent via his/her vehicle computer in real time. Covert LPRs (fixed locations, typically above busy intersections or interstates) are not connected to a computer, therefore they cannot communicate real-time hot list hits. Covert LPRs must be manually checked by Agents, who download the contents of the device into a spreadsheet on the standalone computer at their respective Station. Agents then manually query the downloaded spreadsheet to determine if any hot listed license plates passed by the Covert LPR during the duration of the collection. As mentioned above, Sectors will develop their own procedures for how often Covert LPR information is uploaded to the standalone computer depending on enforcement priority. If Sectors determine that they want to consolidate, share, or connect their standalone systems with each other for operational efficiencies, USBP will complete a new Privacy Threshold Analysis (PTA) for consideration by the CBP Privacy Officer and DHS Chief Privacy Officer.

Sectors must develop their own local standard operating procedures for how to communicate changes to the hot list, specifically to ensure that license plates that are no longer "of interest" are removed from the hot list. USBP Headquarters, in coordination with the CBP Privacy Officer, will direct all USBP Sectors to develop and follow these guidelines. USBP will issue a national policy regarding these requirements to all Sectors within six months of the publication of this PIA. The CBP Privacy Officer will conduct a CBP Privacy Evaluation to determine compliance with this requirement, and compliance with the national policy.

In addition to these locally created and managed hot lists, all license plates of interest are also entered into TECS as a TECS Category 1[12] Record. This allows the case agent to be notified when a vehicle with the license plate of interest is encountered by a CBP-owned and operated LPR. If further investigation shows that the license plate is related to criminal activity, it will be changed to a TECS Record for law enforcement purposes, which makes it available to all other TECS users as an alert if the vehicle or subject is encountered. Once the license plate has been elevated to a TECS Record alert, CBP Officers and Agents operating LPRs at a primary inspection

[12] Alerts identified as a Category 1 are alerts that are in an investigative stage and alert notifications will only be available to the person who entered the information.

location will be notified if a vehicle with that license plate approaches.

Once entered as a TECS Record, CBP Officers or Agents can compare license plate reads at POEs, checkpoints, and state, local, and federal LPR locations to identify patterns suggestive of illicit activity. Such comparisons could be performed randomly or based on existing suspicions pertaining to certain vehicles. Border-centric intelligence derived from these systems solely or in conjunction with the data captured from the already deployed stationary LPR technology provide a new level of awareness heightening CBP Officers and Agents effectiveness in interdicting bulk cash, narcotics, weapons, and enhancing public safety.

If the license plate is no longer of interest, it typically remains as a Category 1 (available only to the case agent, in the investigatory stage), as a record of the case, but is not shared with other TECS users. CBP Officers and Agents will not base law enforcement actions solely off of an alert; it is an investigatory and officer safety tool. As with all law enforcement tools, CBP Officers and Agents must ensure the proper level of suspicion is met before any action is taken with a subject vehicle.

Retention

The Mobile and Covert LPR devices store the license plate reads locally on each device only as long as necessary to transmit to the standalone server. Each Sector or Station is responsible for developing procedures for ensuring the devices are “cleared” or information has been transmitted to the local standalone server, but any information on the device itself should not be considered the official CBP encounter, nor should the reads remain on the device once transmitted to the standalone server.

Hot lists are lists of license plates of interest, based on an indication of criminal behavior or previous encounter. Therefore, hot list information may be retained consistent with the TECS SORN[13] for up to seventy-five (75) years. Sectors or Stations must develop local procedures for how hot lists will be continually updated, and communicated to Agents, to reflect the most accurate list of license plates of interest, including those hot lists that are stored locally on the Mobile LPRs.

The license plate numbers, date, timestamp, and location of the reads as stored on the standalone server will be retained for no more than two years, unless linked to an active law enforcement investigation. After two years, the Sector or Station must manually delete any uploaded reads (per the date and timestamp) that are older than two years. Each Sector or Station must develop procedures to ensure that license plate reads are maintained in accordance with these retention requirements. USBP Headquarters, in coordination with the CBP Privacy Officer, will direct all USBP Sectors to follow these guidelines. USBP will issue a national policy regarding these requirements to all Sectors within six months of the publication of this PIA. The CBP Privacy Officer will conduct a CBP Privacy Evaluation to determine compliance with this requirement,

[13] DHS/CBP-011 U.S. Customs and Border Protection TECS System of Record, 73 FR 77778 (December 19, 2008).

and compliance with the national policy.

Mobile and Covert LPRs do not necessarily connect to a CBP IT system; however, LPR data obtained in support of a CBP investigation or enforcement action seeking to apprehend an individual will be entered in E3[14] or TECS,[15] or both if necessary.

Privacy and Civil Liberties Risks

DHS prohibits the consideration of race or ethnicity in investigation, screening, and law enforcement activities in all but the most exceptional instances. Accordingly, consistent with law and DHS policy, LPR data may not be collected, accessed, used, or retained to target or monitor an individual solely on the basis of actual or perceived race or ethnicity. The following is the Department's official policy[16] on this issue:

> "Racial profiling" is the invidious use of race or ethnicity as a criterion in conducting stops, searches, and other law enforcement, investigation, or screening activities. It is premised on the erroneous assumption that any particular individual of one race or ethnicity is more likely to engage in misconduct than any particular individual of another race or ethnicity. The Department of Homeland Security (DHS) has explicitly adopted the Department of Justice's "Guidance Regarding the Use of Race by Federal Law Enforcement Agencies," issued in June 2003. It is the policy of DHS to prohibit the consideration of race or ethnicity in our daily law enforcement and screening activities in all but the most exceptional instances, as defined in the DOJ Guidance. DHS personnel may use race or ethnicity only when a compelling governmental interest is present, and only in a way narrowly tailored to meet that compelling interest. Of course, race- or ethnicity-based information that is specific to particular suspects or incidents, or ongoing criminal activities, schemes or enterprises, may be considered, as stated in the DOJ Guidance.
>
> Except as noted below, it is DHS policy, although not required by the Constitution, that tools, policies, directives, and rules in law enforcement and security settings that consider, as an investigative or screening criterion, an individual's simple connection to a particular country, by birth or citizenship, should be reserved for situations in which such consideration is based on an assessment of intelligence and risk, and in which alternatives do not meet security needs, and such consideration should remain in place only as long as necessary. These self-imposed limits, however, do not apply to antiterrorism, immigration, or customs activities in which nationality is expressly relevant to the administration or enforcement of a statute, regulation, or executive order, or in individualized discretionary use of nationality as a screening, investigation, or enforcement factor."

[14] *See* DHS/CBP/PIA-012 CBP Portal (E3) to ENFORCE/IDENT, *available at* www.dhs.gov/privacy.
[15] DHS/CBP-011 U.S. Customs and Border Protection TECS System of Record, 73 FR 77778 (December 19, 2008).
[16] Secretary Janet Napolitano, "The Department of Homeland Security's Commitment to Nondiscriminatory Law Enforcement and Screening Activities" (April 26, 2013).

CBP has adopted this policy and includes it in all manuals, policies, directives, and guidelines regarding any activity in which the use of race or ethnicity may arise as a security screening, law enforcement, or investigative criterion. CBP personnel are trained on the policy.

Finally, to the greatest extent possible, CBP will adhere to its guided enforcement policies and procedures and verify the accuracy of vehicle information and any subsequent information obtained from other sources as a result of the LPR data. CBP personnel will take into account the quality, integrity, and age of a given LPR record in assessing its value and use as an enforcement or investigative lead when LPR data is obtained during the course of an investigation or enforcement matter.[17] This requires human evaluation and verification to determine the relevance of LPR data to an active investigation or other authorized law enforcement or homeland security efforts. This also includes visually confirming that the plate characters generated by LPR correspond with the digital image of the license plate in question.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal Government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208 and the Homeland Security Act of 2002 Section 222. As part of its law enforcement program, CBP uses LPR technology, and information derived from the use of such technology, to conduct criminal investigations and civil immigration enforcement actions. As such, this PIA examines, within the construct of the FIPPs, the privacy impact of LPR technology operations.

[17] Secretary Janet Napolitano, "The Department of Homeland Security's Commitment to Nondiscriminatory Law Enforcement and Screening Activities" (April 26, 2013).

1. Principle of Transparency

Principle: *DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.*

All persons entering the United States at and between the ports of entry are subject to monitoring and data collection for operational and situational awareness. CBP posts signs at ports of entry to notify individuals of the monitoring and information collection requirements. LPRs are one of many tools that CBP uses to monitor and screen passengers, vehicles, and cargo that attempt to enter the United States. This PIA also serves to inform the public generally of the presence of LPR technology at the border and the use of this technology to detect and support the apprehension of persons crossing the border illegally.

CBP does not provide advanced notice to individuals encountered between ports of entry because entering the United States without coming through a port of entry is illegal. It is logistically impracticable for CBP to give prior notice to persons seeking to cross the border at a location other than a port of entry; persons seeking to cross the border illegally are informed that their activities in the border area may be monitored and captured for use to enforce the law through the notice provided in this PIA and the associated SORNs.

Privacy Risk: There is a risk that collected images or activities at the border either at or between the ports of entry may include innocent persons or persons who are complying with the law and who have not received notice or provided consent.

Mitigation: Notice for persons at the ports of entry is provided at the ports. Notice for persons in the border area between the ports of entry is found in this PIA. CBP does not obtain consent to use information pertaining to persons crossing the border as it is obliged by statute to ensure the security of the border and to determine the identity and citizenship of all persons crossing the border. CBP signage at the ports of entry informs persons of the video capture and its intended use. CBP recognizes that residents and visitors in areas proximate to the ports of entry and the border may have their images captured incidentally. CBP mitigates this risk by strictly controlling the collection, use, and retention of information through LPRs. Information that is not collected for a law enforcement purpose is deleted and is not used.

Privacy Risk: There is a risk that individuals will not be aware that CBP is collecting their license plate information, either through its own readers or through agreement with the DEA.

Mitigation: This risk is partially mitigated. CBP is publishing this PIA to provide detailed notice to the public about the LPR data it collects. CBP also provides general notice of its collection of license plate information at vehicle border crossing lanes at official Ports of Entry in the TECS

System: CBP Primary and Secondary Processing PIA.[18] In addition, the Border Patrol Enforcement Records (BPER),[19] Border Crossing Information (BCI),[20] and TECS[21] SORNs alert the public that CBP collects "biographic, descriptive, historical, and other identifying data" as well as "travel and other information." The SORNs state that this information is gathered in support of "the identification and arrest of individuals who commit violations of federal criminal laws enforced by DHS" and "the identification, apprehension, and removal of individuals unlawfully entering or present in the United States in violation of the Immigration and Nationality Act, including fugitive aliens." The SORNs also notify the public that data is obtained from commercial and public sources. There remains some risk to transparency, however, in that CBP cannot provide timely notice of its collection of information through Mobile and Covert LPRs, since doing so could reveal the location of a covert device or otherwise compromise law enforcement operations.

2. Principle of Individual Participation

Principle: *DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.*

Generally, travelers entering or exiting the United States by vehicle at land ports of entry are aware of the fact that they are subject to CBP inspection. Although there is no opportunity to opt out of inspection if they intend to cross the border, they are involved in the inspection processes that collect license plate information at both ports of entry and Border Patrol Checkpoints. In the case of Mobile and Covert LPRs, individual participation is less practical, since vehicles in the range of these devices may not be aware that they are in use. CBP cannot provide an opportunity to opt out in such cases, since doing so would alert potential subjects to CBP activity and allow them to evade detection or otherwise interfere with the investigation. Similarly, individuals may not be able to opt out of CBP's use or retention of their data as obtained from the DEA, since such notice is not provided by the DEA at the time of collection.

Individuals seeking notification of and access to records collected during these processes, or seeking to contest their content, may submit a Freedom of Information Act (FOIA) or Privacy Act request to CBP at https://foia.cbp.gov/palMain.aspx, or by mailing a request to:

CBP FOIA Headquarters Office
U.S. Customs and Border Protection

[18] *See* DHS/CBP/PIA-012 TECS System: CBP Primary and Secondary Processing, *available at* www.dhs.gov/privacy.
[19] DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 FR 72601 (October 20, 2016).
[20] DHS/CBP-007 Border Crossing Information (BCI), 81 FR 43462 (December 13, 2016).
[21] DHS/CBP-011 U.S. Customs and Border Protection TECS System of Record, 73 FR 77778 (December 19, 2008).

FOIA Division
1300 Pennsylvania Avenue NW, Room 3.3D
Washington, D.C. 20002
Fax Number: (202) 325-1476

Requests for information are evaluated to ensure that the release of information is lawful; will not impede an investigation of an actual or potential criminal, civil, or regulatory violation; and will not reveal the existence of an investigation or investigative interest on the part of DHS or another agency.

All FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process.

Persons who believe they have been adversely impacted by this program may also contact the CBP INFOCENTER at https://help.cbp.gov/. The CBP INFOCENTER responds to all types of compliments and complaints submitted regarding CBP operations, but typically regarding:

- Experience with CBP arriving in or departing from the United States;
- CBP's Trusted Traveler Programs (Global Entry, NEXUS, SENTRI, GOES, etc.);
- Experience with CBP at a checkpoint or other location patrolled by the Border Patrol;
- Inspections at a general aviation facility (private aviation) or marina;
- Importing/exporting goods or have another issue related to international trade;
- CBP's website, ESTA application, I-94 retrieval, service delays/responsiveness (including lost or missing parcels), general practices and procedures, etc.

Privacy Risk: There is a risk that individuals who are not under suspicion or subjects of investigation may be unaware of or able to consent to CBP surveillance by Mobile or Covert LPRs.

Mitigation: This risk is not mitigated given the purpose of the collection. Providing timely notice of Mobile and Covert LPRs would significantly interfere with and undermine CBP's law enforcement mission. Although the lack of notice and participation poses a privacy risk, especially to individuals who are not under investigation, CBP only accesses PII linked to license plate information when there is circumstantial or supporting evidence linking the vehicle to criminal activity.

Privacy Risk: There is a privacy risk that CBP will incorporate information from external partners into CBP systems without any privacy documentation regarding other federal agency's LPR program(s).

Mitigation: This risk is partially mitigated. Currently, CBP uses ATS-L to query DEA LPR information. All queries must have a nexus to CBP's border enforcement mission. CBP is not ingesting DEA LPR information and will strictly use queries to search DEA LPR data for CBP's border enforcement mission. In addition, using ATS-L to query to DEA LPR system provides a strong audit log capability of all CBP queries.

However, this risk cannot be fully mitigated without corresponding public-facing privacy documentation from external partners regarding the sources of LPR information for their program(s).

Privacy Risk: There is a risk to individual participation in that individuals do not have an opportunity to consent to CBP's retention and use of their license plate data.

Mitigation: This risk is not mitigated given the purpose of the collection. Many areas of both public and private property have signage that alerts individuals that the area is under surveillance; however, this signage does not consistently include a description of how and with whom such data may be shared. Moreover, the only way to opt out of such surveillance is to avoid the impacted area, which may pose significant hardships and be generally unrealistic.

3. Principle of Purpose Specification

Principle: *DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.*

CBP may access and retain LPR data when necessary to carry out law enforcement missions required under numerous authorities, including the Tariff Act of 1930, as amended, and the Immigration and Nationality Act, various criminal and civil provisions, including those in Titles 18, 19, 21, and 31 of the United States Code and associated DHS regulations.

CBP may use LPRs to identify locations and movements of targets and associates believed to be involved in illegal activity in connection with its law enforcement activities. CBP may also use this data to track vehicles suspected of carrying contraband such as smuggled goods. LPR data may be used to identify individuals suspected of involvement in illegal activity during the course of criminal investigations and border security matters and to locate wanted individuals and immigration targets, such as at-large criminal aliens and immigration fugitives. LPR data will be used in conjunction with other information to develop leads to further the enforcement matter and investigation, including identifying new suspects and eliminating others from further consideration. CBP has adopted a systematic process for the analysis of LPR data. Agents begin by identifying a target, de-conflicting the target with other law enforcement agencies, disseminating target information to applicable state, local and federal entities that may encounter the target, communicating the disposition of the target after law enforcement interdiction, and finally analyzing the event to glean intelligence on the subjects involved in illicit activity.

CBP collection of LPR information: USBP is responsible for securing the United States border between the ports of entry. To do this, USBP uses a layered approach that includes patrolling the border itself (including the use of electronic surveillance devices), patrolling nearby areas and neighborhoods where illegal immigrants can quickly fade into the general population, and conducting checkpoints - both stationary and temporary. The authority for this is based on the Immigration and Nationality Act 287(a)(3) and codified in 8 Code of Federal Regulations (CFR) 287 (a)(3), which states that Immigration Officers, without a warrant, may "within a reasonable distance from any external boundary of the United States...board and search for aliens in any vessel within the territorial waters of the United States and any railcar, aircraft, conveyance, or vehicle." 8 CFR 287 (a)(1) defines reasonable distance as 100 air miles from the border. USBP may deploy Mobile or Covert LPRs and capture license plate numbers (front and back) from vehicles traveling in close proximity (within 100 miles) to the border.

CBP collection of DEA LPR information: CBP will only query license plate data to support authorized law enforcement actions as described in the CBP mission (which limits CBP queries to only those cases for which CBP has authority). If the query returns positive encounter data, additional information may be requested by CBP.

Privacy Risk: There is a risk that CBP does not have the appropriate authority to collect LPR information from vehicles traveling down public roads and highways, without passing through a port of entry or Border Patrol Checkpoint.

Mitigation: This risk is mitigated in several different ways depending on how CBP obtains the LPR read. If collected by a CBP-owned Mobile LPR or Covert LPR, the U.S. Border Patrol has unique authorities to collect information up to 100 miles from the U.S. border. If collected by the DEA, CBP will only access and retain LPR information from the DEA that is connected to a CBP hot list or active law enforcement investigation.

4. Principle of Data Minimization

Principle: *DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).*

Only LPR data that is considered relevant or useful to the border inspection, investigation, or law enforcement activity underway will be retained in CBP enforcement systems of record, such as Border Patrol Enforcement Records (BPER)[22] or TECS.[23] The CBP law enforcement

[22] DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 FR 72601 (October 20, 2016).

[23] Examples of such cases are those in which the location of specific vehicles or targets/associates suspected of operating those vehicles may be useful to bringing a law enforcement matter to a conclusion (*e.g.*, closure of a criminal case, arrest of a priority alien).

officer conducting the query will retain the subset of results deemed relevant in the appropriate CBP system of record for the length of time prescribed by the applicable records schedule for that system. Once the LPR data is incorporated into the CBP case file, it and other case file data may be queried and analyzed in other CBP systems established to perform analysis in order to generate additional investigative leads, such as locating targets and linking cases using location information. The CBP LPR data retention framework is as follows:

1. CBP retains investigative information in BPER and TECS for 75 years to ensure the information is available for the life of a law enforcement investigation.
2. For LPR information collected as part of a border crossing event (through a port of entry or Border Patrol Checkpoint), LPR information is retained for 15 years consistent with the BCI SORN.
3. For LPR information collected from Mobile and Covert LPRs, CBP will retain this information in local, standalone computers for no more than two years (unless linked to an active law enforcement matter, then it will be transferred to an enforcement database and stored for 75 years).
4. LPR information will only be stored locally on a Covert LPR device until it is transferred to a standalone database. Data will be stored on the Covert LPR device only so long as necessary to transmit the information to the standalone computer.

CBP will not retain in its records the results of its queries of DEA databases unless the information is determined to be useful in connection with its legitimate law enforcement activities. These limitations and requirements will help to ensure CBP's access to and retention of LPR data are compatible with the purpose for which the data is sought and to minimize the risk of an over-collection of this data.

Privacy Risk: There is a risk that CBP's collection of LPR data may constitute an over collection of sensitive information related to an individual's movements.

Mitigation: This risk is partially mitigated. CBP may collect LPR data over an extended period of time in order to establish patterns related to criminal activity. Accordingly, CBP may collect information related to individuals' movements that may not relate to criminal activity. To mitigate the associated privacy risks, CBP restricts retention of Mobile and Covert LPR data to no more than two years, unless linked to an active law enforcement activity, to ensure that it will not be retained arbitrarily.

Additionally, CBP closely adheres to DHS policy prohibiting the consideration of race or ethnicity in investigation, screening, and law enforcement activities in all but the most exceptional instances. Accordingly, consistent with law and DHS policy, LPR data may not be collected, accessed, used, or retained to target or monitor an individual solely on the basis of actual or perceived race or ethnicity.[24]

<u>Privacy Risk</u>: There is a risk that license plates on a "hot list" will continue to trigger various alerts after the immigration, law enforcement, or national security action has been closed.

<u>Mitigation</u>: Each Sector (or Station) is responsible for developing and maintaining a local "hot list" of license plates of interest. A license plate of interest is typically related to a vehicle or person who is the subject of an active law enforcement investigation. Each Sector (or Station), will maintain its own hot list which is typically a list of the current top ten or twenty license plates of interest. The hot list can change daily, depending on the Sector or Station enforcement priorities.

The hot list will be used in two ways: (a) storage on the device for real time matching and (b) manual query by Agents at the Station. Mobile LPRs (on Agent vehicles) are connected to the Agent's vehicle computer, and therefore can upload the hot list directly to the LPR capture device. If a vehicle on the list passes by the Mobile LPR, it will alert the Agent via his/her vehicle computer in real time. Covert LPRs (fixed locations, typically above busy intersections or interstates) will only store encounters long enough to transmit to a standalone server. Sectors must develop their own local standard operating procedures for how to communicate changes to the hot list, specifically to ensure that license plates that are no longer "of interest" are removed from the hot list.

5. Principle of Use Limitation

Principle: *DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.*

CBP collects license plate information for several purposes, and the uses of license plate information varies by purposes. For automated license plate reader collections, the primary purposes for collection is officer safety, law enforcement, and to create a border crossing record. By collecting a license plate image before a vehicle reaches the primary inspection point at a port of entry or a Border Patrol Checkpoint, CBP Officers and Agents have time to check for outstanding enforcement issues or officer safety concerns (such as a previous port-runner, or armed and dangerous subject) associated with the license plate. This gives the CBP Officers and Agents invaluable time to take adequate safety and precautionary measures when approaching the subject vehicle.

[24] Secretary Janet Napolitano, "The Department of Homeland Security's Commitment to Nondiscriminatory Law Enforcement and Screening Activities" (April 26, 2013).

CBP also collects license plate information at primary to determine if the license plate is associated with any outstanding law enforcement actions or investigations. If so, CBP Officers and Agents will take appropriate action either by apprehending the individual or referring the subject to secondary inspection for additional review. Lastly, the license plate information is retained in TECS as a border crossing record, regardless of whether there is associated law enforcement activity associated with the license plate number, as part of the subject's border crossing information.

For Mobile and Covert LPRs, the purpose for collection is strictly law enforcement and investigatory. All license plate information collected from Mobile and Covert LPRs is searched against hot lists of license plates of interest to the various Sectors and Stations, for law enforcement investigation and action. All other license plate information captured is deleted by the Sectors and Stations within two years of collection.

Privacy Risk: There is a risk that CBP will use LPR data for a purpose other than that for which it originally collected the information.

Mitigation: To mitigate the risk of purpose specification, CBP will only use LPR data in support of its law enforcement investigations consistent with its authorities, and access to this data is restricted to individuals with a legitimate need to know. CBP employees only use LPR data in compliance with applicable laws, policies, and directives. CBP trains users about appropriate collection and use procedures before providing access to a particular system. Failure to comply with these guidelines is a violation of CBP's Code of Conduct and may subject an employee to disciplinary action, including termination of employment or prosecution.

Privacy Risk: There is a risk that the DEA will share CBP license plate data from TECS without CBP's knowledge or consent.

Mitigation: This risk is partially mitigated. Pursuant to the signed DEA TECS User Agreement, except as required by U.S. law, information received pursuant to the MOU will not be disseminated outside of DHS or vetted DEA users without the express prior-written consent of the providing party unless it is a level 1 TECS record as described above. If the DEA receives a request from a third party for CBP LPR information (including requests under FOIA or the Privacy Act), the DEA must consult with CBP on how to respond to the request and, if appropriate, will refer the request to CBP for response.

6. Principle of Data Quality and Integrity

Principle: *DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.*

LPR information is just one of many sources of investigative information, and CBP personnel are generally prohibited from taking enforcement action predicated solely on LPR data. In any investigative matter, CBP personnel recognize the importance of taking action based on data that is accurate, relevant, timely, and complete, to the extent possible. CBP Officers and Agents perform other database checks to ensure that any action taken is based on the most current information available about the vehicle, location, and subject of the case. Existing legal and policy constraints against the misuse of PII are designed to ensure that LPR information used during enforcement matters is accurate. LPR-specific training will emphasize these requirements.

Privacy Risk: There is a risk that CBP Agents using Mobile LPRs will rely on outdated hot lists that are stored in the device.

Mitigation: This risk is partially mitigated. Each Sector (or Station) is responsible for developing and maintaining a local "hot list" of license plates of interest. A license plate of interest is typically related to a vehicle or person who is the subject of an active law enforcement investigation. Each Sector or Station, will maintain its own "hot list," which is typically a list of the current top ten or twenty license plates of interest. The hot list can change daily, depending on the Sector or Station enforcement priorities. Sectors must develop their own local standard operating procedures for how to communicate changes to the hot list, specifically to ensure that license plates that are no longer "of interest" are removed from the hot list.

Privacy Risk: There is a risk that a license plate read may be incomplete or inaccurate due to environmental conditions (weather or visibility) or damage to the plate itself, resulting in the misidentification of a vehicle and its occupants.

Mitigation: This risk is partially mitigated. LPRs are typically operating in an open environment and although CBP takes steps to ensure that stationary readers are positioned to minimize environmental interference, the impacts cannot be fully mitigated. In addition, CBP personnel visually confirm the LPR reads to mitigate the risk of error. CBP mitigates the potential for harm by ensuring that officers do not take action based on LPR reads alone.

Privacy Risk: There is a privacy risk that CBP will incorporate LPR information from external partners into CBP systems without knowing the sources or fidelity of the LPR information.

Mitigation: This risk is partially mitigated. CBP will not share LPR information via streaming service with external partners unless the partner publishes a public-facing PIA describing its License Plate Reader program(s) and corresponding information technology system controls. However, CBP will query external partner information to the extent there is a border security nexus for the query, and may include the LPR information as part of a CBP enforcement record if relevant to CBP's border security or law enforcement mission(s).

This risk cannot be fully mitigated without corresponding public-facing privacy documentation from external partners regarding the sources of LPR information for their program.

7. Principle of Security

Principle: *DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

The automated LPR information is maintained within the TECS system and is protected in accordance with the TECS security controls.

The Mobile and Covert LPR devices are approved by the CBP Office of Information and Technology (OIT) and included on the CBP Technical Reference Model, which lists all available and prohibited technology for use within CBP. Use of the Mobile and Covert LPR technology is currently restricted to U.S. Border Patrol mission functions. Per the technical reference model, the standalone computer that USBP uses to store Mobile and Covert LPR information will not connect to a CBP network. Additionally, the Mobile and Covert LPR data collected will not be transmitted back to the device vendor at any time.

Privacy Risk: There is a risk that an unauthorized individual may access LPR data without a legitimate need to know.

Mitigation: This risk is mitigated. Only authorized CBP Officers and Agents with a need to know, typically in the intelligence units, will have access to the Mobile and Covert LPR readers or information. All users must be vetted for authentication prior to being granted access. The Mobile and Covert LPR devices themselves are also password protected and cannot be accessed without the corresponding connection device back to the standalone computer. The standalone computer is also password-protected and only accessible by designated CBP Officers and Agents with a need to know in their respective Sectors.

8. Principle of Accountability and Auditing

Principle: *DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.*

Automated LPR information is maintained in TECS, therefore the security and auditing controls from the TECS system platform ensure that automated LPR information is used appropriately. TECS users are classified into the following categories: general system users; supervisors; system control officers; systems maintenance personnel; and security administrators. Every new and existing user of TECS is assigned a system control officer. The system control officer is responsible for the user's profile record and assigns the role(s) (*i.e.*, a CBP Officer) and the accessible service functions (*i.e.*, Secondary Inspection) within that role. CBP manages the assignment of system control officers so that the system control officer may assign only functions that the system control officer has authority to use, as well as authority to assign. User accounts are reviewed periodically and certified annually to ensure that these standards are maintained. TECS actively prevents access to information for which a user lacks authorization, as defined by the user's role in the system, location of duty station, and job position. Multiple attempts to access information without proper authorization will cause TECS to suspend access automatically.

The TECS platform automatically generates audit logs that capture all users' activity. Audit logs are captured at the time of logon and throughout the user's session. The audit logs consist of a journal of the user's data requests or queries into the TECS datasets, and contain the user ID, date and time, and the location and activity performed, such as the query terms. These audit logs allow system administrators to respond to "user activity" requests from the CBP Office of Professional Responsibility to investigate abuse of the TECS Platform.

Users are required to have and maintain, at minimum, a background investigation status and successfully complete the TECS Security and Privacy Awareness training annually to gain and retain access and certification to information on the TECS Platform. Functions required to perform job duties are reinstated after a user completes the recertification.

Privacy Risk: In addition to the license plate information stored in TECS, USBP will store the reads from Mobile and Covert LPRs in local, standalone databases at the various Sectors and Stations without the same robust auditing and accountability procedures.

Mitigation: There are no auditing or accountability measures built into the standalone database, however the risk is partially mitigated because it is a) not connected to the network, and b) only a limited number of users have access to the specific computer secured at the local Sector or Station. All USBP users have completed a background investigation and are sworn law enforcement officers. Any unauthorized use of the LPR information will result in disciplinary action.

Privacy Risk: There is a risk that CBP LPR information may be used in a manner inconsistent with the DEA sharing of license plate reader data MOU.

Mitigation: This risk is mitigated. Pursuant to the MOU, the DEA shall work with CBP to develop a review standard and protocol to validate the technical safeguards regulating the streaming flow of CBP LPR data. The DEA shall certify to CBP every six months that it is appropriately filtering the streaming flow of CBP LPR data and only retaining CBP LPR data that is responsive to a DEA lookout or alert.

The DEA shall provide CBP on a monthly basis with a statistical report on the number of DEA lookouts or alerts that were triggered based on the CBP LPR data provided through the streaming service. This report shall include the total number of alerts triggered in the previous month, the number of license plates that were encountered by CBP on four (4) or more occasions in the previous month, and the number of license plates that were encountered by CBP on seven (7) or more occasions in the previous month. The DEA and CBP points of contact may, by mutual written agreement, alter the requirements or time period for this periodic reporting.

Any modifications to the MOU must be reviewed and approved by the CBP Office of Chief Counsel and the CBP Privacy Officer.

Responsible Officials

Antonio Trindade
Associate Chief, Enforcement Systems
U.S. Border Patrol
U.S. Customs and Border Protection

Debra L. Danisek
CBP Privacy Officer
Privacy and Diversity Office
U.S. Customs and Border Protection

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security