Privacy Impact Assessment

for the

CBP License Plate Reader Technology

DHS Reference No. DHS/CBP/PIA-049(a)

July 6, 2020

Homeland Security

Abstract

The U.S. 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. In 2017, CBP published a Privacy Impact Assessment (PIA) describing its use of commercially available fixed and mobile license plate reader technology. CBP is conducting this Privacy Impact Assessment (PIA) update to provide public notice of CBP's use of license plate reader data procured from commercial vendors.

Overview

U.S. Customs and Border Protection (CBP) is responsible for securing the borders of the United States while facilitating lawful international trade and travel. To meet its vast mission requirements, CBP relies on a variety of law enforcement tools and techniques for law enforcement and border security. One such tool is license plate reader (LPR) technology, which consists of high-speed 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. LPR technology 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.

Reason for the PIA Update

CBP published a Privacy Impact Assessment (PIA) in 2017 detailing the privacy risks associated with its use of LPR technology. The 2017 PIA only discussed LPR reads obtained from equipment owned and operated by CBP; at the time, CBP did not access commercially available license plate images and vehicle locations. Since that time, CBP has taken steps to procure access to commercial license plate databases.[2] Accordingly, CBP is updating this PIA to provide

[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.
[2] CBP's operational use of the information in the commercial database will commence on or after the date of publication of this PIA and not before.

additional notice to the public and assess the unique privacy risks associated with the use of a commercial vendor license plate database.

CBP plans to use the Automated Targeting System (ATS)[3] to access commercially available LPR information from a vendor service in order to provide CBP law enforcement personnel with a broader ability to search license plates of interest nationwide. A number of commercial services collect and aggregate LPR data from both private and public sources and make it available on a fee-for-service basis. Typically, LPR vendors collect license plate image information from private businesses (e.g., parking garages), local governments (e.g., toll booth cameras), law enforcement agencies, and financial institutions via their contracted repossession companies. The LPR commercial aggregator services store, index, and sell access to the images, along with the time and location of the collection. CBP will only have access to images from U.S. based cameras that are part of the commercial aggregator's services.

CBP has identified a number of benefits from the use of commercially aggregated LPR data for its law enforcement and border security mission. The data can: 1) identify individuals and vehicles that may need additional scrutiny when attempting to cross the border; 2) enhance both officer and public safety by enabling enforcement actions to occur in locations that minimize the inherent dangers associated with border enforcement encounters; and 3) help resolve matters that might otherwise be closed for lack of viable leads. In support of these activities, CBP has acquired access to LPR data via an Application Programing Interface (API) to query data aggregated and made available to CBP users by commercial LPR vendors. CBP accesses the commercial LPR database through the contract provider providing on-demand federated queries through ATS. ATS does not ingest the data; instead, similar to the other existing commercial data interfaces (such as LexisNexis), CBP has created a web service through which authorized ATS users may create vehicle displays that present vehicles of possible interest, query historical LPR data, and use advanced analytics for enhanced review and analysis.

Results of queries via the API are stored in ATS, as well as other appropriate CBP systems, such as TECS,[4] the Intelligence Reporting System Next Generation (IRS-NG), and the Analytical Framework for Intelligence (AFI),[5] if the information is determined to be useful in connection with a legitimate law enforcement or border security mission. This retention will be consistent with the National Archives and Records Administration (NARA) retention schedule as specified in the relevant System of Records Notice (SORN).[6]

---

[3] CBP is publishing a separate update to the ATS PIA to provide notice of the commercial license plate data available through the system. See DHS/CBP/PIA-006(e) Automated Targeting System, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[4] LPR data may identify individuals that need additional scrutiny at the border, in which case the LPR information will be used in TECS to create a lookout record.

[5] DHS/CBP/PIA-010 Analytical Framework for Intelligence, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[6] *See* DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012); DHS/CBP-011 U.S. Customs and

Location-based commercially aggregated data creates a number of privacy risks. CBP has taken steps to mitigate these concerns by ensuring that access to this sensitive information is strictly limited and auditable and by ensuring that all uses of commercially available LPR information are consistent with CBP law enforcement and border security authorities. CBP has limited access to the commercial LPR information through a newly created role within ATS that requires a multi-level approval process. CBP will routinely audit queries of the commercial service to ensure queries are only associated with ongoing enforcement or border security activities. CBP personnel will use LPR data as a tool to further heightened suspicion and generate leads predicated on a relevant CBP mission.

CBP users are permitted to query commercially available LPR information to identify locations and movements of *already identified* subjects and associates believed to be involved in illegal activity in connection with CBP's law enforcement or border security mission. CBP may also use this data to track vehicles suspected of carrying contraband, such as smuggled goods. Personnel may also use LPR information in conjunction with other law enforcement and/or targeting information to develop leads to further the enforcement matter, including identifying associates of possible concern and eliminating other individuals from further consideration. In addition, CBP may use this information to identify individuals or vehicles that may need additional scrutiny when crossing the border. CBP will not use commercially available LPR data to generate new leads or identify new patterns.

CBP will only use LPR data to identify locations and movements of targets and associates believed to be involved in illegal activity in connection with law enforcement or border security mission. For example, LPR data is particularly useful in enforcement matters in which CBP is attempting to identify or locate members of criminal organizations abetting the movement of terrorists, weapons, narcotics, or smuggled aliens. It is also useful in the detection and identification of tactics, trends, and patterns used by those organizations engaging in illicit activity at the border or attempting to harm the country. Users query the commercial LPR database using a license plate number, address of reader, or make or model of a vehicle the user wants to locate within ATS. The database returns any responsive records, which may include any or all of the above data elements. The search results will contain all LPR reads from the vendor, with a primary focus on reads occurring within the last 30 days. The search results will be maintained temporarily in the cache. Caching of data eliminates the need to repeat the same queries over a short period of time. Query results are typically cached for a minimum of four hours, but not more than twenty-four hours, after which they are automatically deleted from ATS.

CBP users will create "events" in the ATS-Targeting Framework (TF) to store relevant LPR query responses. ATS-Targeting Framework "events" show what open research projects

---

Border Protection TECS, 73 FR 77778 (December 19, 2008); DHS/CBP-024 Intelligence Records System (CIRS) System of Records, 82 FR 44198 (September 21, 2017), *available at* https://www.dhs.gov/system-records-notices-sorns.

belong to each user. CBP users will determine whether the query responses are relevant to their research, and if so, may save the query results to the relevant "event." No query responses will be automatically saved. If an LPR result is not relevant to law enforcement or border security missions, users may not save the query result to an event with ATS-TF. All query results that are not uploaded to "events" are automatically deleted from the cache within twenty-four hours. Query responses that are stored in ATS-TF "events" contain only information that is relevant, such as license plate number of a vehicle and the location of a vehicle. CBP users are required to review and validate each item on a "display list" at least once yearly; however, users will be required to update "display lists" as needed when matters are resolved or when the location of a vehicle is no longer of value to law enforcement or border security mission. As stated below, CBP management or oversight personnel will review displays on a quarterly basis and verify those LPR reads that are still relevant to CBP's law enforcement or border security mission.

CBP users may query LPR data through the AFI search functionality.[7] If the query results are relevant to CBP's law enforcement or border security mission, the results will be added to an AFI Project. An AFI Project will allow CBP users to expand their research, while adding additional data sources to compile connections between a vehicle and an address know for criminal activity. This information may help CBP to identify individuals, or vehicles, involved in criminal activity who may need additional scrutiny when attempting to cross the border or to identify and locate suspects involved in terrorist activities. CBP users who also have access to IRS-NG will have the capability to query LPR data. If LPR data is relevant to CBP's law enforcement or border security mission, CBP users will have the capability to add the results to an IRS-NG Workspace where users are able to add additional data while conducting research. IRS-NG Workspaces are limited on viewing to select groups until a user decides to publish an Intelligence Product. IRS-NG users are able to produce Intelligence Products that could be posted in AFI, where CBP personnel are able to use this information to assist with CBP's law enforcement or border security mission. A CBP user will determine if LPR data is relevant to CBP's law enforcement and border security mission and if LPR data is determined to be not relevant, it will be automatically deleted from the system, after no more than a twenty-four-hour cache.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[8] 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. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure

[7] For more information on AFI, see DHS/CBP/PIA-010 Analytical Framework for Intelligence, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[8] 5 U.S.C. § 552a.

that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[9]

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.[10] 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[11] and the Homeland Security Act of 2002 Section 222.[12] As part of its law enforcement program, CBP uses information derived from the use of commercial LPR 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 data.

1. Principle of Transparency

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.

CBP is publishing this updated PIA, as well as a recent addendum to the ATS PIA, to inform the public about LPR data CBP can access through a commercial provider. Both documents provide a detailed description of what CBP is collecting, storing, and retaining, and the privacy risks that are associated with this activity. In addition, CBP has the ATS SORN provides public notice that CBP collects information from commercial data providers.

The data CBP obtains from the commercial provider originates from a variety of sources, including private companies and other government agencies. Neither CBP nor the commercial provider can provide notice at the point of collection, nor does it have the authority to require the entity deploying the readers to provide such notice.

Privacy Risk: There is a risk that individuals may not be aware that CBP may access data associated with their license plates. This risk is enhanced by the fact that CBP may access reads captured anywhere in the United States, outside of the border zone in which CBP enforcement activities take place.

---

[9] 6 U.S.C. § 142(a)(2).
[10] *See* Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06, "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security," *available at* https://www.dhs.gov/privacy-policy-guidance.
[11] 44 U.S.C. § 3501 note.
[12] 6 U.S.C. § 142.

Mitigation: This risk cannot be fully mitigated. Neither CBP nor the commercial provider controls the LPRs at the source, so neither can ensure that the subject of the read is aware of the collection, or aware that the information may eventually be accessible to CBP. Because CBP cannot provide notice at the point of collection, it is publishing this PIA, as well as the ATS PIA and SORN, to provide detailed notice to the public about the LPR data it collects.

2. Principle of Individual Participation

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.

Individual participation is not practical for most LPRs 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 it is not involved at the point 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://foiaonline.gov/foiaonline/action/public/home, or by mailing a request to:

CBP FOIA Headquarters Office
U.S. Customs and Border Protection
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 include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process. CBP can only provide records that are controlled by CBP. CBP will only include a small subset of the commercial vendor data in CBP systems. Only the information in CBP systems may be responsive to FOIA requests.

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 (e.g., Global Entry, NEXUS, SENTRI, GOES);
- 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.

To the extent that a record is exempted in a source system, the exemption will continue to apply. Because of the law enforcement nature of ATS, DHS has exempted portions of this system from the notification, access, amendment, and certain accounting provisions of the Privacy Act of 1974. These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records with appropriate exemptions in place.

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 access to their license plate information through a commercial database.

Mitigation: This risk cannot be fully mitigated. CBP cannot provide timely notice of license plate reads obtained from various sources outside of its control. 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. Although the lack of notice and participation poses a privacy risk, especially to individuals who are not under investigation, CBP helps reduce the impact of this risk by only accessing license plate information when there is circumstantial or supporting evidence to a lead and does not retain any information not associated with a law enforcement event.

3. Principle of Purpose Specification

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, the Immigration and Nationality Act, and various criminal and civil provisions, including those in Titles 18, 19, 21, and 31 of the United States Code and associated DHS regulations.

CBP maintains LPR information in support of its law enforcement and border security mission under the DHS/CBP-006 Automated Targeting System SORN.[13] As reflected in the SORN, commercial data aggregators are a record source category and used for the purpose of law enforcement and/or researching information regarding an individual.

LPR records in support of CBP's law enforcement and border security mission to record information on individuals to whom CBP has issued detentions and warnings are covered under the DHS/CBP-011 TECS SORN.[14]

LPR records collected by CBP to support CBP's law enforcement and border security mission are covered by DHS/CBP-024 CBP Intelligence Records System.[15] This SORN notified the public that data is obtained from commercial data providers, among other sources, in the course of intelligence research, analysis, and reporting.

Consistent with these authorities and the SORNs listed above, CBP may use commercial LPR data 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. Commercial 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. Commercial 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.

Privacy Risk: There is a risk that CBP does not have the appropriate authority to collect commercially available LPR information from vehicles operating away from the border and outside of CBP's area of responsibility.

Mitigation: This risk is mitigated. Similar to its use of other commercially available information, CBP only accesses this information relevant to its law enforcement and border security mission and will only retain information associated with those who cross the border and those who may be linked or connected to a person of law enforcement interest, connected to potentially criminal or other illicit activity, or for identifying individuals or entities of concern. Queries will only be associated with ongoing enforcement or border security activities. Should a CBP personnel use LPR information outside of these parameters, the auditing and accountability

[13] *See* DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.
[14] *See* DHS/CBP-011 TECS, 73 FR 7778 (December 19, 2008), *available at* https://www.dhs.gov/system-records-notices-sorns.
[15] *See* DHS/CBP-024 CBP Intelligence Records System, 82 FR 44198 (September 21, 2017), *available at* https://www.dhs.gov/system-records-notices-sorns.

requirements will discover any misuse.

4. Principle of Data Minimization

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).

CBP will be able to query five years of historical data to allow CBP personnel to conduct additional analysis and research regarding border security or law enforcement matters and to access sufficient historical data to identify trends, patterns, and potentially viable information. CBP will not retain in its records the results of its queries of LPR databases unless the information is determined to be useful in connection with its legitimate law enforcement or border security mission. These limitations and requirements will help to ensure CBP's access to LPR data is compatible with the purpose for which the data is sought and to minimize the risk of an over-collection of this data.

LPR data will be updated on a continuous basis from the commercial provider and the updates will be reflected when queried by ATS. CBP will retain the results of its queries of the LPR data in ATS or other appropriate CBP system (e.g., TECS or AFI) if the information is determined to be useful in connection with its legitimate law enforcement or border security mission. This retention will be consistent with the NARA retention schedule as specified in the relevant SORN. The purpose of these limits is to allow CBP users seeking to conduct additional analysis and research regarding border security or law enforcement matters access to sufficient historical data to identify trends, patterns and potentially viable information or leads, while not retaining data so long as to result in the unnecessary or excessive acquisition of information.

Privacy Risk: There is a risk that CBP's use of commercial LPR data may constitute an over collection of sensitive information related to an individual's movements. For example, LPR data from third party sources may, in the aggregate, reveal information about an individual's travel over time, or provide details about an individual's private life, leading to privacy concerns or implicating constitutionally-protected freedoms.

Mitigation: This risk is partially mitigated. CBP may access LPR data over an extended period of time in order to establish patterns related to criminal activity; however, CBP has limited its access to LPR data to a five-year period in an effort to minimize this risk. CBP will not retain in its records the results of its queries of LPR databases unless the information is determined to be useful in connection with its legitimate law enforcement or border security mission. These limitations and requirements will help to ensure CBP's access to 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. DHS privacy policies require CBP to assess privacy risks in connection with the use of LPR

technology and data and follow the DHS FIPPs to the extent possible. DHS civil liberties policies support the evaluation of the risks to individual rights and liberties as a result of the use of LPR technology. DHS and CBP are committed to safeguarding PII, upholding civil liberties, and reducing potential risks posed by this technology.

5. Principle of Use Limitation

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 identified a number of benefits from the use of LPR data from a commercial provider for its law enforcement and border security mission. Knowing the previous location(s) of a vehicle can help determine the location of subjects of criminal investigations, illicit activity, or aliens who illegally entered the United States, and thus facilitate their interdiction and apprehension. In some cases, the availability of this data may be the only viable way to find a subject. This LPR data can also show the previous movements of a subject, which may help CBP law enforcement personnel plan to apprehend while maximizing safety to the public and the officers. The vendor maintains daily refresh updates to their data to ensure the information is accurate and reliable. CBP will use LPR data from commercial providers to identify connections between a vehicle and an address known for criminal activity, which may help identify individuals involved in criminal activity, permit CBP to identify those individuals who, or vehicles that, may need additional scrutiny when attempting to cross the border, or to identify and locate suspects involved in terrorist activities.

CBP is implementing a structure that will mitigate privacy and civil liberties concerns raised by the commercial acquisition and CBP's use, storage and maintenance of LPR-related data, taking into account the growth in the availability of LPR data and the potentially sensitive information it can reveal. This structure will encompass:

1. Limited Role-Based User Access Controls: Access to commercially available LPR information will be provisioned through the CBP Entitlement System where a new entitlement role has been specifically created for this access. CBP users who require access to this sensitive dataset will proceed through a multi-level approval process. If it is determined that commercially available LPR information access is appropriate for the requestor's targeting and analytical efforts the request may be granted, or if deemed inappropriate, denied. Once LPR access is granted, CBP will provide the user an email authorizing access to LPR data, reiterating that improper use of this data may result in disciplinary action, and describing appropriate use of accessing LPR data on CBP systems laid out within this ATS PIA addendum. CBP management will ensure that requestors have met the training requirements, described below.

2. Training: CBP will require all personnel permitted to access LPR data via commercial subscription to take mandatory training for data security, privacy, information assurance, and records management on an annual basis. ATS user roles will be granted and used only for those who meet the training requirements. User roles are restricted and audited, with access predicated on a "need to know." Through user access control "entitlements", all ATS users are only permitted to access information from the source systems to which they have already been granted access. System access is managed by the ATS Entitlement System and reviewed annually to ensure the users that have access to the LPR data are recertified by a government lead.

3. Specified Purpose: When logging into ATS, AFI or IRS-NG, authorized CBP users will see a description of the permissible uses of the system and will require a user to consent affirmatively to the requirements of accessing information on a U.S. Government system with no reasonable expectation of privacy. Each time a CBP user logs into ATS, the user must agree to the terms and conditions set forth in a splash screen before performing any query. The splash screen describes the agency's permissible uses of the system and data, and requires the user to affirmatively consent to these rules by selecting a button before proceeding. The following rules apply to the splash screen:

    - The splash screen appears at each logon event; and
    - Users must affirm their understanding of the rules of behavior before they are able to complete the login process and commence a query.

4. Timeframe for Query of Historical LPR Data and Retention of Results: Privacy and civil liberties concerns associated with historical searches of LPR data increase the longer the data is held by the vendor and made accessible for query. However, operational necessity may require CBP to access information sufficient to establish patterns of criminal activity over time as part of ongoing analysis or criminal investigation or to identify the movement or location of priority organizations or known associates. Therefore, CBP has determined that personnel may query five years of historical commercial LPR data to allow CBP personnel to conduct additional analysis and research regarding border security or law enforcement matters and access to sufficient historical data to identify trends, patterns, and potentially viable information. CBP will implement a cap within CBP systems to only allow CBP users to access LPR data within a five-year period from the date of the query. CBP will only retain the results of its queries of the LPR data in ATS or other appropriate CBP systems (i.e., TECS or AFI) if the information is determined to be useful in connection with its legitimate law enforcement or border security

mission. This retention will be consistent with the NARA retention schedule as specified in the relevant SORNs. CBP must manually retain the results of its queries of the LPR data that is determined to be useful in connection with its legitimate law enforcement or border security mission, while all other query results are automatically removed from the cache within twenty-four hours.

5. Use of Displays: CBP will use the capability to store license plate queries in the form of a "display" in ATS, whereby any new read of a plate on the display will result in notification to CBP. This capability will assist in the identification of a vehicle's location in near real-time, which will contribute to law enforcement efforts to apprehend individuals whose location may be connected to the vehicle's location or to know if a vehicle linked to illicit activity is approaching a port of entry. While automatic notification that an individual subject is on the move could raise privacy and civil liberties concerns, such notification also serves an important law enforcement interest. To help reduce the potential intrusiveness of this technique, CBP policy will require displays to be updated once the enforcement matter is resolved or the individual is no longer a subject of interest. Upon creation, users will also receive notice on the importance of promptly removing license plate numbers from displays to avoid gathering LPR data without adequate justification. Users will be prompted via system notification to reexamine the entirety of their displays on a regular basis and, at a minimum, annually. Should users fail to meet this requirement, the displays will expire from the system. CBP management will review displays on a quarterly basis and verify those that are still relevant to CBP's law enforcement and border security mission.

6. Audit: ATS will provide an audit trail of each query that is made and by whom it is made. Specifically, the audit logs will capture: 1) the identity of the user initiating the query; 2) the license plate number used to query the LPR data; 3) the date and time of the inquiry; and 4) the results of the user's query. The audit trail should be generated electronically and will need to be available to, and reviewed by, CBP management or oversight personnel quarterly or more frequently to ensure the data is being used appropriately. For auditing purposes, ATS stores all query parameters, but not the query results. The vendor does not have access to these audit trails.

7. Accountability: All ATS users must undergo privacy training and obtain approval from CBP management and the ATS system owner before gaining access to ATS. ATS performs extensive auditing that records the search activities for all users. ATS has role-based access which is restricted based on a demonstrated "need to know." Data may only be accessed using the CBP network with encrypted passwords and user sign-on functionality. CBP users with access to commercially available LPR information are required to complete annual security and data privacy training and

their usage of the system is audited to ensure compliance with all privacy and data security requirements. CBP management will be held accountable for ensuring personnel with access to LPR data sets are properly trained and use LPR data appropriately. Periodic reviews of audit logs will confirm this is occurring. CBP management will review displays on a quarterly basis and verify those that are still relevant to CBP's law enforcement and border security mission. Auditing would be the responsibility of CBP through ATS where detailed audit logging will be implemented. DHS and/or CBP integrity offices will investigate any anomalous activity uncovered in the audit logs and CBP management will impose appropriate disciplinary action if misuse is discovered.

DHS defines PII as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual. The use of LPR data received from a commercial provider and used within ATS is considered PII because the license plate information is linkable to an individual. CBP recognizes there are potential privacy risks and impacts on the individual rights associated with the use and retention of LPR data.

Privacy Risk: LPR data may be inappropriately accessed or disseminated.

Mitigation: This risk is partially mitigated. To assist in securing LPR data against unauthorized access, use, and dissemination, CBP has set out specific requirements that limit that amount of LPR information that is made available. These requirements included creating a new ATS entitlement role where a user will need to demonstrate a clear "need to know" in order to be provisioned to commercially available LPR information, retention of the data consistent with the retention schedules of ATS, TECS, IRS-NG and AFI as reflected in the relevant SORNs; internal policy controls that ensure queries are conducted only for law enforcement or border security purposes; and strong auditing requirements. CBP will require all personnel permitted to access LPR data to take mandatory training for data security, privacy, information assurance, and records management on an annual basis. When access to LPR data is granted, CBP will provide the user an email authorizing access to LPR data and stating the appropriate use of accessing LPR data on CBP systems laid out within this ATS PIA addendum. CBP further mitigates this risk by ensuring CBP only shares information with agencies outside of DHS consistent with the Privacy Act, including the routine uses it has published in the relevant SORNs (e.g., TECS, ATS, and AFI).

6. Principle of Data Quality and Integrity

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

As with all commercial data sources, LPR information is just one of many sources of investigative information, and CBP personnel are generally prohibited from taking enforcement action predicated solely on commercial 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 commercial LPR information used during enforcement matters is accurate.

Privacy Risk: There is a risk that a license plate read accessed through a commercial vendor 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. While CBP cannot control the quality of the license plate data aggregated by the commercial vendor, Officers and Agents are trained to evaluate all available information and assess for accuracy and reliability. CBP further mitigates the potential for harm by ensuring that officers do not take action based solely on commercially available LPR data.

Privacy Risk: LPR data may accurately identify the location of a vehicle, but there is a risk that it may not accurately identify the whereabouts of the person that CBP is seeking.

Mitigation: This risk is partially mitigated. While LPR information can only accurately locate a vehicle and not a person, CBP Officers and Agents are trained to evaluate all of the available information, which includes other database checks, to ensure that any action taken is based upon reliable information. CBP further mitigates the potential for harm by ensuring that officers do not take action based solely on commercially available LPR data.

7. Principle of Security

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.

Any commercial LPR information that is responsive to CBP queries is maintained in ATS or the appropriate CBP system and is protected in accordance with the system security controls. Access to commercially available LPR information will be provisioned through the CBP Entitlement System where a new entitlement role has been specifically created for this access. CBP users who require access to this sensitive dataset will proceed through a multi-level approval

process. If it is determined that commercially available LPR information access is appropriate for the requestor's targeting and analytical efforts the request may be granted, or if deemed inappropriate, denied. Once CBP grants LPR access, CBP will provide the user an email authorizing access to LPR data, reiterating that improper use of this data may result in disciplinary action, and describing appropriate use of accessing LPR data on CBP systems laid out within this ATS PIA addendum. CBP management will ensure that requestors have met the training requirements, described below.

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

Mitigation: This risk is mitigated. Strict access controls in ATS and other CBP systems ensures that only authorized users can view the commercial LPR data.

8. Principle of Accountability and Auditing

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.

ATS maintains robust audit trails and makes them available to appropriate CBP personnel for review. ATS will record all transactions and queries of LPR data in immutable audit logs at the individual authorized-user level and these logs are subject to review at any time by CBP oversight offices and system managers as appropriate. Specifically, system audit logs must capture: 1) the identity of the user initiating the query; 2) the license plate number used to query the LPR system; and 3) the date and time of the inquiry. This data will also be captured, thereby enhancing the usefulness of the audit trail data. The primary goal of maintaining audit logs is to deter and discover any abuse or misuse of LPR data. Any abuse or misuse of LPR data will be reported and subject to disciplinary action, as appropriate.

Before being granted access to LPR data, authorized CBP users must complete training that describes all of the above policy requirements and associated privacy, civil rights, and civil liberties safeguards. This will supplement existing mandatory training required of all CBP personnel on data security, data privacy, integrity awareness, and records management.

Privacy Risk: LPR data from a commercial provider is not subject to internal DHS auditing and accountability controls; therefore, there is a risk these controls may not occur or be as robust as they would be if the vendor's system were internal to DHS. There is a risk that LPR data may be accessed routinely (even when not needed) or retained for periods longer than necessary without appropriate controls and oversight.

Mitigation: This risk is mitigated. This risk can be managed by preventing over-collection and retention of the information. CBP will implement internal policies and training emphasizing the requirement to query and use LPR data only when in support of a law enforcement or border

security purpose. Audit trails will capture sufficient usage data to allow the identification of CBP users who do not comply with these policies. CBP users will be required to review and validate each item on a display at least once yearly; however, employees will be required to update the displays as needed when matters are resolved or when the location of a given vehicle is no longer of law enforcement value. The fact that CBP users will have to associate queries with ongoing enforcement or border security purpose in order to perform the queries will provide an enforcement mechanism for these requirements.

In addition, to ensure that LPR information is appropriately accessed, ATS and the vendor will capture information about the query of a license plate number. The primary goal of maintaining audit logs is to deter and discover any abuse or misuse of LPR data. Any abuse or misuse of LPR data will be reported and subject to disciplinary action, as appropriate.

Responsible Officials

Courtney T. Ray
Acting Associate Chief, Enforcement Systems
U.S. Border Patrol
U.S. Customs and Border Protection
(202) 325-4601

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

Approval Signature

[Original signed copy complete and on file with the DHS Privacy Office]

_____

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717