Drug Enforcement Administration

Privacy Impact Assessment
for the
National License Plate Reader Program (NLPRP)
and DEA Special Intelligence Link (DEASIL)

Issued by:
James Robert Bryden
DEA Senior Component Official for Privacy

Approved by: Brian Young
Deputy Director (Acting)
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: December 20, 2024

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The Drug Enforcement Administration's (DEA) National License Plate Reader Program (NLPRP) System is a law enforcement tool developed and used by DEA to enforce Title 21 authorities by facilitating the investigation of drug trafficking, bulk cash smuggling and other illegal activities associated with the drug trade. The NLPRP *Network* is the DEA-owned network of license plate reader (LPR) camera equipment on high-level drug and money trafficking corridors, that can also be connected to other LPR cameras placed on public roadways nationwide by other federal agencies; state, local, tribal law enforcement partners; and other entities with a special law enforcement jurisdiction.

At DEA's El Paso Intelligence Center (EPIC), the DEA's NLPRP System organizes the images taken by the DEA's NLPRP Network**.** The NLPRP System contains known license plates, and can be accessed through the DEA Special Intelligence Link (DEASIL) interface for authorized investigative searches. The DEASIL interface can be accessed for searches by DEA and also by state, local, tribal and other federal law enforcement partners to assist investigations within the statutory authority of partner agencies occurring on high-level drug and money trafficking corridors and other public roadways throughout the United States.

In 2019, the DEA published a Privacy Impact Assessment (PIA) describing the privacy risks associated with its use of LPR technology and the controls established to minimize impact on personal privacy and civil liberties. This PIA is being updated to inform the public about the changes with the NLPRP System functionality since 2019 and inform the public about new functionalities that are being considered for implementation, and the controls that will be established to protect personal privacy and civil liberties. To the extent this PIA includes discussion of NLPRP Network camera hardware, it will not extend to any LPR camera hardware owned by partner agencies.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

The transportation of illegal substances via public roadways presents a significant challenge to law enforcement agencies tasked with intercepting and stopping these activities. The transportation of illegal substances by vehicle presents significant challenges for law enforcement personnel, as criminals use a variety of methods to conceal their activities. This

makes it difficult to detect and intercept these vehicles, resulting in an ongoing flow of drugs into the United States and drug proceeds going out the United States, contributing to the ongoing drug epidemic. Additionally, the risks associated with such transportation are substantial and pose a significant threat to public safety as they can lead to high-speed chases avoiding arrest, accidents, and other dangerous situations. Furthermore, the use of vehicles for transporting illegal drugs increases the risk of violence for police engaging in traffic stops, as criminals involved in these drug-related activities are often armed and dangerous.

To address the threats raised by drug trafficking, bulk cash smuggling, and other criminal activities on high-level drug trafficking corridors and on other public roadways throughout the United States, the DEA developed the NLPRP Network. The NLPRP is a collection of LPR cameras and equipment owned by the DEA to collect--either directly using DEA cameras and authorities, or as photographed and provided to DEA by other federal, state, local, tribal and special jurisdiction law enforcement agencies (partner agencies) under their authorities--images of all vehicle license plates passing through certain locations to assist law enforcement personnel during drug-related investigations.

Under the terms of Memoranda of Understanding (MOUs) facilitating law enforcement partner agency participation, LPR images captured by non-DEA equipment under the authorities of those partner agencies are provided to DEA under partner agency authority and incorporated into the NLPRP System database under DEA authority (21 U.S.C. § 801 *et seq*.). These images are available to be queried for a designated period by both DEA and non-DEA law enforcement personnel authorized to access and use the system. The NLPRP enters into these sharing MOUs either directly with Federal, State, local or tribal law enforcement agencies or with regional hubs. A regional hub is a state, local, tribal law enforcement agency, or a High Intensity Drug Trafficking Area (HIDTA) that gathers LPR information from contributing law enforcement agencies within the region. These contributing agencies transmit their LPR data to servers maintained by regional hubs pursuant to their individual MOUs, which stipulate that this data may be shared with the NLPRP system. MOUs between the NLPRP and law enforcement agencies and regional hubs include provisions to ensure that the dissemination of LPR data complies with applicable laws and regulations, restricts access to official law enforcement use, and incorporates other measures to protect civilian liberties and individual privacy. Currently, the NLPRP has established MOUs with over 250 law enforcement agencies and hubs. Templates for these MOUs can be found in Appendix 1 and 2 of this PIA.

The NLPRP System is an investigative tool that can be combined with other tools, investigative methods, and techniques used by DEA personnel to assist in their investigations of drug trafficking, bulk cash smuggling, and other associated criminal offenses. DEA personnel, along with other law enforcement personnel at partner agencies, can access the NLPRP System through the DEA Special Intelligence Link, also known as DEASIL. This access supports their drug-related investigations, as well as other investigations such as traffic stops and missing person cases, within the framework of their partner agency authorities and missions.[1]

[1] Such other law enforcement purposes are compatible with the purpose for which the information was collected. See, e.g., routine use (a) in DEA-008, *Investigative Reporting and Filing System,* 77 FR 21808, 21809 (4-11-2012).

An LPR consists of a high-speed camera, or cameras, and related equipment mounted on either vehicles or fixed locations. Fixed location cameras are stationary and are only used on public roadways or elsewhere with the permission of a property owner. In contrast, mobile readers are only utilized on official law enforcement vehicles or platforms. The system automatically, and without human intervention, photographs all vehicles that come into range of an LPR camera. Once a photograph is taken, the system scans the image using Optical Character Recognition (OCR) technology to identify the license plate number and, in some cases, the state of registration. The cameras are positioned to photograph license plates in the front and rear of the vehicle. However, depending on the site and the camera field of view, the photographs may also capture other portions of the vehicle or an overall image of the vehicle, such as make and model or the environment surrounding the vehicle, including passersby, other vehicles' license plates, or other numbers in the surrounding environment. Although unintended, the photograph may also capture interior portions of the vehicle visible through a vehicle's window, including images of the occupants.

Photographs taken by LPR cameras, together with other data points such as the date and time the license plate was recognized, the owner of the LPR camera, the type of LPR camera, the GPS coordinates of the LPR camera, the lane of the vehicle's travel, and the direction of the vehicle's travel are then transmitted to the NLPRP System and becomes a searchable LPR record in the system. DEA-owned LPR cameras are directly linked to the NLPRP system. LPRs cameras owned by law enforcement entities other than DEA may be connected to the NLPRP by direct link, a virtual private network, or a server to which both DEA and the other law enforcement agencies have access. An LPR record establishes a particular vehicle is at a particular place at a particular time and permits the linking a license plate with the name of person to whom it is registered. The NLPRP System is designed to delete all files older than 90 days by default.

The NLPRP System operates through another DEA system called SOURCE License Plate Reader (LPR) to ingest new LPR images and metadata. This system is an externally facing component of the DEA's information technology infrastructure. It provides a secure DEA-controlled area for ingesting telecommunications data from cameras owned by DEA, as well as those owned by partner agencies as is set forth in the respective Memoranda of Understanding with each agency. Once the data is received, a separated enclave immediately and securely transfers data to the appropriate internal DEA location for further processing.

Authorized NLPRP users from DEA and partner agencies can access and retrieve LPR records through the DEASIL interface, which serves as the IT infrastructure for the NLPRP gateway portal. DEASIL consolidates and streamlines users' access to the NLPRP system by providing secure, direct, remote, and internal and external connectivity via a web display of the data collected. "Internal" access refers exclusively to DEA employees accessing DEASIL from the DEA's Firebird internal network, while "external" access pertains to authorized users from other partner agencies connecting via the external Internet through a secure web browser. The

DEASIL application is a Sensitive But Unclassified (SBU) system that is hosted on the Speedway/Unclassified (Speedway/U) infrastructure managed by DEA[2].

To retrieve LPR records, authorized users make investigative requests (detailed below) to determine whether an LPR camera has recognized a license plate of interest within the previous 90 days. Additionally, users can set up an alert for a license plate of interest so that they will be notified if an LPR captures and recognizes an image of the subject license plate in the NLPRP System within the next 30 days. Further, the NLPRP System automatically conducts deconfliction on behalf of the user to determine whether a particular license plate is also of interest in a different investigation.

Dissemination of license plate records in the NLPRP System to DEA's law enforcement partners across the country occurs through authorized access via DEASIL. To the extent that the NLPRP System may be considered a system of records, DEA shares LPR records (please see Section 3.1 below) with its partner agencies consistent with DEA's routine uses as published in relevant SORNs or with other exceptions provided in the Privacy Act. See System of Record Notice JUSTICE/DEA-008 and JUSTICE/DEA-022, as amended.[3] Further, all law enforcement agencies involved in the NLPRP Network have information sharing agreements with the DEA, detailing the parameters for using and further sharing LPR records that equipment collects. DEA and its law enforcement partners have also instituted policies and procedures to protect individual privacy and civil liberties when using the NLPRP System. Information gathered through the LPR camera network is maintained in the NLPRP System for no more than 90 days from the date it is captured before it becomes unavailable to users and deleted from the system.

NLPRP System Capabilities.

Investigative Request. An investigative request is a query to obtain LPR records regarding the recent location history of a license plate. To initiate an investigative request, authorized users must possess:

(A) both a legitimate investigative need and a reasonable, articulable suspicion that a specific license plate is linked to criminal activity (and is memorialized by the user selecting from a list of reasons provided by the system), or

(B) must require the information for lawful purposes connected to a traffic stop, or

(C) authorized users may request such information if the license plate is connected to a missing person's case (including Silver and Amber Alerts) even where reasonable articulable suspicion does not exist.

---

[2] Speedway/U is covered by separate privacy documentation.

[3] JUSTICE/DEA-008, Investigative Reporting and Filing System, 77 Fed. Reg. 21808 (Apr. 11, 2012), 82 Fed. Reg. 24151 (May 25, 2017) and JUSTICE/DEA-022, El Paso Intelligence Center (EPIC) Seizure System (ESS), 71 Fed. Reg. 36362 (Jun. 26, 2006), 82 Fed. Reg. 24147 (May 25, 2017).

To submit an investigative request, users must provide:

1) the complete or partial license plate number or other number of interest;[4]

2) the search type (match type) required to obtain relevant data;

3) the maximum number of results requested, ranging from 100 to all responsive data;

4) the rationale for the request;

5) the agency and case number associated with the request; and

6) if the request is being made on behalf of another individual, the requester must provide the person's name and agency.

There are two available match types for the search: "exact" and "soundex." To have an "exact" match, the OCR read of the license plate must be precisely the same characters as those entered by the user, without any additional or missing characters. A "soundex" search utilizes pre-determined rules to provide data that is similar to the license plate number of interest while maintaining the exact order of characters. For instance, if the license plate in question is "ABC L23," a "soundex" search might return the license plate number "ABC 123." Moreover, administrative users have the ability to perform "no read" and "contains" searches. A "no read" search enables administrative users to receive data regarding information obtained when the OCR technology was unable to read any characters to try to determine the reasons for the lack of a read. A "contains" search allows for responsive license plate numbers to have extra characters before and/or after the characters entered by the user. The System's Rules of Behavior require users to visually inspect the license plate images to confirm that the license plate photographed in any result is the one being investigated or otherwise relevant to the investigation.

In addition, when making an investigative request, the user may enter the following information to narrow the request: 1) time zone of LPR cameras (so that only images with associated times from the time zone of interest are included in the response); 2) start date and time for the time period to be searched; 3) end date and time for the time period to be searched; 4) a state of interest (so that only data obtained in that state will be searched); and 5) a location of interest (so that only data obtained in that location will be searched).

After submitting the investigative request, the user will receive responsive LPR records based on the entries made. The response may include the following information for each vehicle recognized with a license plate number that fits the entered criteria: 1) a percentage-based degree of confidence indicating how closely the recognized license plate matches the license plate number of interest, as determined by the OCR technology; 2) the license plate number recognized by the OCR technology; 3) the vehicle's registration state shown on the license plate, as determined by the OCR technology; 4) the sighting state; 5) the sighting location; 6) the roadway name, including the lane of the roadway; 7) the direction of travel; 8) the date(s) and time(s) of recognition; 9) one or more images of the license plate, vehicle, and/or

[4] In the remainder of the document, for simplicity, the phrase “license plate number” is used to refer to license plate numbers and other numbers of interest.

surrounding environment; and 10) the identification name/number of the LPR camera. Additionally, a user can conduct an interval search related to a sighting of interest. An interval search enables a user to examine all images and data obtained from the same sighting location for a certain period of time around the time of a sighting of interest.

In exigent circumstances (information or allegations of forcible felonies where death or great bodily harm to a person or person(s) has occurred or will likely occur based on the actions of the target suspect), users can request a wildcard search. The EPIC standards require such a requestor to provide detailed and specific reasons based on current knowledge or observations that indicate the search is necessary given the situation at hand, based on a reasonable articulable suspicion. With the authorization of a DEA Senior Executive Service-level supervisor (the EPIC Director), a limited number of administrative users are able to conduct a wildcard search. When conducting a wildcard search, a user can indicate, by inserting an asterisk, places among the characters entered where there may be unknown characters. The user will receive in response images and data relating to license plates containing the characters entered as well as any additional characters in the locations of the asterisks. These wildcard requests are thoroughly reviewed by El Paso Intelligence Center (EPIC) management to ensure the request complies with relevant laws and regulations and individual and civil liberties are protected. EPIC keeps records of all requests, relevant emails, approvals, documents and DEASIL exigent search results.

The information gathered provides law enforcement with vital investigative information regarding the locations of target vehicles. The photographic images and data collected by the NLPRP enables law enforcement officers to confirm or discount information already gathered from sources, to locate vehicles, and to gather additional investigative information. Additionally, when a user receives responses to an investigative request, the user can perform an interval search that allows the user to look at all images and data obtained from the same sighting location as a selected response(s) for a certain period of time around the time of a sighting of interest. This feature allows users to confirm or discount source information, locate additional target- or accomplice-associated vehicles, and gather additional investigative information.

Alerts. An authorized user can set up alerts for license plates of interest. To set up an alert, users must have an investigative need and reasonable articulable suspicion that a particular license plate is involved in criminal activity. Users may also set up an alert when a particular license plate is involved in a missing person case (even if there is no reasonable articulable suspicion of criminal activity). When an alert is set up for a license plate of interest, the user will be notified if the license plate is recognized by an LPR camera in the system within the next 30 days.

When setting up an alert, the user must enter the following information: 1) whether the alert is being set up for the user or on behalf of another person, whose name and agency must be identified; 2) the user's reason for setting up the alert; 3) the state of the vehicle's registration; 4) the license plate number; 5) an alert name (a free-text field for the user to provide a name for the alert); 6) the associated case number; 7) whether the associated investigation is active or not; 8) the alert type, which indicates whether or not the user would like law enforcement officials who see the vehicle of interest to interdict the vehicle; 9) the primary case agent's full

name and office phone number and a phone number at which he or she is available at all times; 10) a second case agent's full name and office phone number and a phone number at which he or she is available at all times; 11) the primary case agent's supervisor's full name and office phone number and a phone number at which he or she is available at all times; and 12) at least one email address or phone number to which responsive information will be sent. The user setting up the alert may also enter the following information: year, make, model, color, and other description of the vehicle, the registered owner's name, a home phone number for the primary case agent, second case agent, and/or supervisor, additional email addresses and/or phone numbers to which responsive information will be sent, and remarks, a free-text remarks field in which a user can enter additional information related to the targeted vehicle.

Once the alert is set up, if, within the next 30 days, a license plate is recognized by an LPR camera in the NLPRP system that, based on the OCR technology scan of the license plate, may be the license plate of interest, a notification is sent, within approximately 10-15 seconds, to the user. The match between the OCR read of the recognized license plate need not be an exact match to the license plate number of interest for a notification to be sent out, but the system's Rules of Behavior require requestors visually inspect all license plate results to confirm relevance.

Further, when viewing the captured information, the recipient receives a warning that the recipient should verify, by reviewing the photographs taken, that the license plate photographed is actually the one of interest. The warning also cautions that the OCR read alone cannot be the sole basis for taking further enforcement actions.

The recipient will have access to the following information: 1) the image or images of the license plate, vehicle, and/or surrounding environment; 2) the license plate number recognized, as determined by the OCR technology; 3) the state of the vehicle's registration as shown on the license plate, as determined by the OCR technology if determined by the OCR technology; 4) the location of detection; 5) the time of detection; 6) the roadway name; 7) the direction of travel; 8) the identification name/number of the LPR camera; 9) the alert type, as entered by the user who created the alert; 10) the year, make, model, color, and/or other description of the vehicle, as entered by the user who created the alert if entered by the user; 11) the registered vehicle owner's name, as entered by the user who created the alert if entered by the user; 12) the primary case agent, second case agent, and supervisor's names and contact information, as entered by the user who created the alert; 13) the name of the user who created the alert; 14) the alert name as entered by the user who created the alert; 15) the expiration date of the alert; 16) the associated case number; 17) one or more identification numbers for the alert or associated data file, generated by the NLPRP system; 18) any remarks entered by the user who created the alert if entered by the user; and 19) the notification history relating to the license plate of interest, including the number of times the license plate has been recognized, the first date and time on which the license plate was recognized, and the most recent date and time on which the license plate was recognized.

The near real-time nature of NLPRP alerts also provides an opportunity for a tactical law enforcement response to specific investigative or operational situations. As the result of an alert, officers who are mobilized for a tactical law enforcement response may receive notification that the subject vehicle is approaching their location. Alternatively, if officers learn

the location of the subject vehicle, but are not themselves in that area, they may request a law enforcement response from officers in the immediate geographic area of the subject vehicle.

Deconfliction. DEASIL automatically conducts "alert deconfliction" whenever an investigative request or alert is set up. In the context of DEASIL, "alert deconfliction" refers to a process where, if multiple users create an active alert for a particular license plate number, or if a user requests an investigation on a license plate for which another user has already set up an alert; both users will receive an email notification indicating the "overlap." This notification is generated automatically by the DEASIL system and includes each user's name, agency, and contact information. The purpose of this notification is to enable users to contact one another and deconflict investigations if necessary. Other than the queried license plate information, no other investigative information is shared through this automatic notification. This deconfliction feature helps law enforcement agencies coordinate their investigations effectively.[5]

DICE Deconfliction Interconnection. The DEA's Deconfliction and Information Coordination Endeavor (DICE) is an information system developed to assist Federal, State, local, and tribal law enforcement agencies in deconflicting investigative information by accessing the DEA Analysis and Response Tracking System (DARTS),[6] DEA's internal deconfliction information system. Deconfliction is a method to determine if other law enforcement agencies are investigating the same target as the user. DICE and DARTS users have been capable of querying license plate numbers that have been previously entered into these systems by other DICE and DARTS users. Where two users have entered matching information on separate inquiries, each user will receive a conflict notification, including the name, agency, and contact information of the other user. DICE Deconfliction is an interconnection with the NLPRP System that alerts DICE and DARTS users querying license plate information about the existence of matching license plate information on the NLPRP system within the last 90 days.

Retention. Users are authorized to retain queried results from investigative requests or alerts that they determine are relevant to their investigation. Users are required to save and maintain the information in the appropriate agency's investigative case file system in a manner consistent with the user's agency records retention policies. DEA users may only retain information from the NLPRP that they determine has relevance to investigative or enforcement activities, and that they place a relevant LPR record in the appropriate DEA investigative records file contained within DEA's Investigative Reporting and Filing System. The records retention schedule for these records is described in JUSTICE/DEA-008, which is published in the Federal Register, 77 FR 21808 (April 11, 2012), available at https://www.justice.gov/opcl/doj-systems-records.

---

[5] The previous 2019 PIA described an interconnection between DEASIL and a separate DEA system used to conduct case deconfliction, titled the Deconfliction and Information Coordination Endeavor (DICE). This interconnection enabled DICE users to simultaneously query DEASIL when conducting "investigative deconfliction" in DICE. This interconnection was discontinued in 2019. However, DEA is contemplating adding a similar interconnection with DICE and the DEA Analysis and Response Tracking System (DARTS). This is discussed in detail in the "Upcoming Updates to the NLPRP System" below.

[6] DICE and DARTS are separate from NLPRP, requiring separate privacy documentation.

Users. LPR records in the NLPRP System are shared with personnel from Federal, State, local, tribal law enforcement agencies, and special law enforcement jurisdictions through access to DEASIL. Individuals who may access and retrieve LPR records from the NLPRP through DEASIL include Law Enforcement Officers and law enforcement support personnel, including intelligence analysts, dispatchers, and government attorneys working on criminal investigations. DEA users must undergo a background investigation and have an official need for accessing the NLPRP System to obtain access. Non-DEA users seeking access to the NLPRP must be vetted by EPIC before being granted access to the NLPRP. Applicants requesting access must undergo a background screening required by DEA and provide personally identifying information and information about their employing agency. The applicant's Supervisor and the respective agency's security coordinator must authorize the applicant to access the system and confirm that the individual requesting access has an official need for accessing the NLPRP system to perform their duties. These checks are performed by the EPIC User Access Management (UAM) Team, which is the same team that conducts background screening and access approval for all information systems in use at EPIC.

Before being given access to the DEASIL application, all users are required to read and comply with the NLPRP's Rules of Behavior (ROB), receive training for using the system, and recertify periodically for continued access. DEA users are also required to complete annual security awareness training. Users who violate the rules of behavior or security procedures may be denied access to the NLPRP or face more severe civil/criminal penalties, if applicable.

Access to specific system administrative information within the DEASIL application is restricted by assigned roles, which include Regular User, Maintenance User, System Administrator, Security Administrator, and User Access Manager. Regular Users may only conduct investigative requests and alerts, as described above. Maintenance Users have IT-related access for system management and maintenance. System Administrators, Security Administrators, and User Access Managers (either government employees or DEA contractors) have expanded permissions for administrative purposes. These three roles make up the three major components of the NLPRP IT administration for the DEASIL application and the NLPRP System. The System Administrators are responsible for maintaining and operating NLPRP as a whole, including backing it up and its recovery. Security Administrators are responsible for viewing, monitoring, and archiving security logs and audit trails. User Access Managers are responsible for adding, changing, or deleting users and their access privileges. DEA contractors are given specific roles that align with the authorized scope of their work. DEA contractors must adhere to information security and privacy guidelines stipulated in their contracts, which bind them to the Privacy Act and other DEA policies.

Authorized users may access and retrieve information from the DEASIL application for themselves or on behalf of other law enforcement personnel. For example, an authorized user may access information in the NLPRP for a co-worker who is conducting an investigation, or a member of another agency who has called the authorized user and provided information regarding the need to conduct an investigative request or set up an alert.

Authorized users may also contact the EPIC Watch[7] to request information from DEASIL. EPIC Watch is a group of DEA personnel at EPIC who can conduct investigative requests and set up alerts on behalf of authorized NLPRP users. In addition, EPIC Watch personnel may provide to the authorized user the following information regarding the license plate of interest: date(s)/time(s) of license plate sightings in the last 90 days, whether there is an existing alert for the license plate, and the point of contact relating to that alert.

Upcoming Updates to the NLPRP System.

DEA is considering system improvements that will enhance the effectiveness of the NLPRP system while continuing to prioritize the protection of personal privacy and civil liberties. The following improvements are intended to strengthen our capabilities and ensure the responsible use of technology in the service of public safety. We understand the public's interest in the use of these technologies and the potential implications for personal privacy and civil liberties. We remain committed to transparent communication and ensuring that these tools are utilized responsibly, respecting individuals' privacy rights while enhancing our ability to protect public safety. Please note that the details outlined in the below future updates to the system are subject to change. DEA will update this PIA to reflect any such changes to maintain the public informed about the latest developments and our ongoing efforts to balance technological innovation with privacy protections.

New Auditing Features. DEA is committed to enhancing its auditing system by implementing advanced automated features when available that will further secure sensitive information and maintain compliance with applicable laws and regulations. The updated system will automatically track changes to role assignments, role creation, and role deletions, reducing manual monitoring and ensuring timely detection of unauthorized modifications. It will employ automated analysis tools to identify unusual activities, unauthorized access attempts, or potential security threats in audit logs, alerting Security Administrators for further investigation. User actions within the DEASIL application, such as data access, failed login attempts, password changes, and account lockouts will be automatically tracked, generating alerts for any suspicious activities. The system will automatically identify users whose access privileges require review, ensuring that only authorized personnel have access to sensitive information based on their job responsibilities. Automated alert capabilities will notify multiple levels of Security Administrators of potential security threats or unauthorized access attempts in real-time, enabling a prompt response and mitigating potential damages. By integrating these automated features into the existing auditing system, NLPRP will enhance its security posture, reduce manual efforts, and proactively address potential privacy risks and unauthorized access attempts.

Multi-Factor Authentication (MFA). MFA is a multi-layered, integrated authentication process that significantly increases the security posture when employed. MFA consists of a two-factor authentication process (i.e., two different methods of authentication) that integrates with an Identity Access Management (IAM) solution. The DEA will be updating DEASIL access with

[7] The EPIC Watch provides tactical intelligence in response to law enforcement agency requests for information in support of Federal, State, local or tribal field law enforcement investigations.

an MFA authenticator which will provide an additional layer of security to protect the DEASIL from unauthorized access. These one-time passwords are valid only for a short duration, significantly reducing the risk of unauthorized access, even if a user's password is compromised. The implementation of MFA through a commercial vendor authenticator application ensures compatibility and reliability, while offering a user-friendly and secure method to safeguard the NLPRP system against potential threats.

Training Requirements. The DEA is committed to enhancing the training requirements for all DEASIL authorized users to ensure the highest level of data security, privacy, and compliance with policy requirements. While the current training focuses on the use of DEASIL, DEA will develop a comprehensive training packet to supplement the existing training. The updated training program will concentrate on essential topics such as data security, data privacy, integrity awareness, records management, policy requirements, and associated privacy, civil rights, and civil liberties safeguards. This comprehensive approach will equip personnel with the knowledge and skills necessary to ensure that accessed LPR data is relevant to ongoing investigative and enforcement activities. By updating the training requirements, DEA aims to strengthen the responsible use of sensitive information, maintain the highest standards of data protection, and uphold privacy, civil rights, and civil liberties.

LPR Data Sharing with U.S. Customs and Border Protection. DEA is seeking to partner with the U.S Customs and Border Protection (CBP) to add CBP LPR cameras located at United States Ports of Entry (POE) to the NLPRP network. CBP's POE LPR cameras will photograph license plates in the front and rear of the vehicle. These cameras may also capture location, date and time of collection, the type of LPR camera, the GPS coordinates of the LPR camera, the lane of the vehicle's travel, the direction of the vehicle's travel, and the environment surrounding the vehicle. CBP-owned cameras will be connected to the NLPRP system and feed data in real-time. With this addition, authorized users will be able to conduct investigative requests or set-up alerts through DEASIL and determine if a CBP LPR camera has recognized a license plate of interest within the previous 90 days. DEA will sign an information sharing agreement prior to sharing information with CBP. The connection of CBP LPR cameras, however, will not extend to any other LPR data CBP maintains from commercial vendors. See, DHS/CBP/PIA-049 CBP License Plate Reader Technology Privacy Impact Assessments (2017 & 2020).

Compliance with State and Local Laws. In recent years, LPRs have become increasingly prevalent in the United States, leading to the implementation of laws addressing the use of LPR data in several states. Some states have enacted laws regulating data retention periods, prohibiting the use of LPR system for certain enforcement actions, and implementing limitations on data sharing. Currently, the NLPRP system cannot receive data from States with more restrictive laws than its current settings.[8] To ensure compliance with these laws, DEA is developing system policies and settings specific to each state. This implementation will be documented via Memorandum of Understanding (MOU) with the State's agency provider.

[8] For instance, certain jurisdictions have enacted legislation limiting how long LPR data can be retained. Some of these retention periods are shorter than NLPRP's retention standard of up to 90 days. Additionally, certain states have introduced legislation restricting sharing or using LPR data for specific law enforcement activities.

Once implemented, the NLPRP system will then be configured to manage data in compliance with specific state requirements, even when state laws are more restrictive than NLPRP's default settings.

Geospatial Interface. A geographical interface is a visual representation of geographical data on a digital platform. In the context of the NLPRP system, a geographical interface will allow authorized users to interact with and analyze spatial data, such as locations, boundaries, roadways, and other geographical features to enhance data utility and user experience. A geospatial interface enhances situational awareness by visualizing captured license plates' locations on a map, revealing spatial patterns to better understand vehicle movement. This capability will allow users to integrate and fuse LPR data with other geospatial datasets (i.e., road networks or crime locations) and other sources of information to provide a more holistic view of a situation, leading to deeper insights and understanding of correlations between vehicle movements and other geographic features. Ultimately, the geospatial interface's ability to present NLPRP data in a spatial context leads to improved law enforcement decision-making. By visualizing and analyzing LPR data spatially, users can identify trends, prioritize resources, and devise more enforcement strategies.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority		Citation/Reference
X	Statute	5 U.S.C. § 301; 44 U.S.C. § 3101 21 U.S.C. § 801 *et seq.*
	Executive Order	
X	Federal Regulation	28 C.F.R. §§ 0.100 and 0.101
X	Agreement, memorandum of understanding, or other documented arrangement	DEA has MOUs for sharing LPR information with Federal, state, local, tribal law enforcement agencies, and other entities with a special law enforcement jurisdiction. All MOUs are based one of two DEA MOU templates with some differences negotiated by the parties. See Appendix for example MOU templates.
	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is

provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C and D	See remarks (*) and (***) at the end of the table. Also include information input by users from State, Local, Tribal law enforcement.
Date of birth or age	X	C and D	See remarks (*) at the end of the table.
Place of birth	X	C and D	See remarks (*) at the end of the table.
Gender	X	C and D	See remarks (*) and (**) at the end of the table.
Race, ethnicity or citizenship	X	C and D	See remarks (*) and (**) at the end of the table.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers	X	A, B, C and D	All license plates in view of LPR are collected
Personal mailing address	X	A, B, C and D	See remarks (*) at the end of the table.
Personal e-mail address	X	A, B, C and D	See remarks (*) and (***) at the end of the table. Also includes information input by users from State, Local, Tribal law enforcement.
Personal phone number	X	A, B, C and D	See remarks (*) and (***) at the end of the table. Also includes information input by users from State, Local, Tribal law enforcement.
Medical records number			
Medical notes or other medical or health information	X	C and D	See remarks (*) at the end of the table.
Financial account information			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C and D	See remarks (*) at the end of the table.
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C and D	LPR only captures location where license was photographed; no continuous or practical intermittent tracking capabilities.
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C and D	See remarks (**) at the end of the table.
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Scars, marks, tattoos**		C and D	See remarks (**) at the end of the table.
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A, B	Also includes users from State, Local, Tribal law enforcement.
- **User passwords/codes**	X	A, B	Also includes users from State, Local, Tribal law enforcement.
- **IP address**	X	A, B	Also includes users from State, Local, Tribal law enforcement.
- **Date/time of access**	X	A, B	Also includes users from State, Local, Tribal law enforcement.
- **Queries run**	X	A, B	Also includes users from State, Local, Tribal law enforcement.
- **Content of files accessed/reviewed**			
- **Contents of files**			
Other types (please list all other types of identifying information collected and describe as completely as possible):	X	A, B	Users may include other relevant information in the alert section's free text field that may include other, unknown personally identifying information.

* The LPR cameras do not collect this information. Although not common, an NLPRP user could enter this information into the free-text remarks field when creating an alert. If the license plate of interest is recognized by a LPR in the system within the 30 days after the alert is created, designated recipients of the alert will be notified, and the notification will contain the information that was entered in the remarks field.

**In addition to potentially being included in the remarks field of an alert, this information may be able to be derived by viewing a photographic image of a license plate that also captures the image of a person. NLPRP does not include facial recognition technology.

***The LPR cameras do not collect this information. Rather, an NLPRP authorized user will enter this information for himself or herself, a secondary agent, and/or a supervisor when using the NLPRP.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	

Phone		Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other Federal entities	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): Note: some information comes from requestors via phone calls or online input					

Non-government sources:					
Members of the public		Public media, Internet		Private sector	
Commercial data brokers					
Other (specify):					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X		X	Only authorized users within DEA may access the NLPRP through DEASIL and images are shared among DEA personnel on a need-to-know basis.
DOJ Components	X		X	Only authorized users within DOJ may access the NLPRP through DEASIL and images are shared among other DOJ personnel on a need-to-know basis.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Federal entities	X		X	Only authorized users within non-DEA/DOJ federal entities may access the NLPRP system through DEASIL. Such users must agree to access and use the system only for the purpose described in Section 2. Participating Federal agencies also agree to sharing of this data as described via MOUs incorporating uses listed in Section 2.
State, local, tribal gov't entities	X		X	Only state, local and tribal law enforcement personnel who are authorized users may access the NLPRP system through DEASIL. Such users must agree to access and use the system only for the purpose described in Section 2. Participating agencies also agree to sharing of this data as described via MOUs incorporating uses listed in Section 2.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			LPR records could be used as evidence during criminal court proceedings.
Private sector				
Foreign governments	X			Any sharing of LPR images/metadata with foreign governments would be done outside the system—there is no direct access. Sharing of LPR data would be done only according to a relevant Routine Use using digital or hard copies taken from case files or downloaded from the NLPRP system.
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or

for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

NLPRP information will not to be released to the public for Open Data purposes on data.gov.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

All data collected from by the LPRs is done to acquire information relevant to law enforcement purposes. Because this system is used for a law enforcement purpose and may contain information related to criminal and civil investigations, it is not feasible or advisable to provide notice to individuals at the time their information is collected by the system. Therefore, no contemporaneous notification is provided to any individual of data collected by each DEA LPR camera. A very general public notice of the categories of investigative information that DEA collects in connection with mission-related activities is listed in SORN JUSTICE/DEA-008, *Investigative Reporting and Filing System* 77 Fed. Reg. 21,808 (April 11, 2012), and SORN JUSTICE/DEA-022, El Paso Intelligence Center Seizure System, 71 Fed. Reg. 36362 (Jun. 26, 2006), published in the Federal Register. DEA-008 and DEA-022 also describe DEA purposes for collecting such kinds of information. Additionally, LPR images matches become DEA law enforcement records retained pursuant to DEA-008 and DEA-022 are exempt from the Privacy Act's individual notice requirement. DEA is unable to provide timely notice of collection of information through LPRs because doing so could reveal the location of a covert device or otherwise compromise law enforcement operations.

As explained in Section 2, DEA does not retain license plate data that has been linked to a person beyond 90 days unless the individual is connected to a criminal investigation. Additionally, DEA shares information with participating agencies pursuant to information sharing MOUs in a manner consistent with the routine use disclosure provisions in the Privacy Act, which is published in SORN DEA-008.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Generally, individuals do not have the opportunity to consent to the collection, use or dissemination of information gathered through the LPR system. Obtaining consent would be unfeasible and would thwart law enforcement investigations. Granting individuals the ability to participate in decisions regarding the collection, use, dissemination or retention of their LPR data would substantially compromise and undermine DEA's law enforcement mission. As a result, DEA does not solicit consent for the collection or use of LPR data. In addition, as

specified in Section 5.1, DEA law enforcement records pursuant to SORN DEA-008 are exempt from the Privacy Act requirement mandating individual notice for information collection. Information is exclusively collected in locations where equipment installation has been authorized by the property owner and on public roadways, where individuals generally do not possess a reasonable expectation of privacy.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Individuals may exercise their rights to access DEA records under the Freedom of Information Act (FOIA) or the Privacy Act. However, information contained on investigative records may be redacted consistent with applicable FOIA exemptions. Additionally, DEA-008 is subject to certain exemptions to the access and amendment provisions of the Privacy Act, as described and authorized in 28 C.F.R. Section 16.98.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls.** **Provide date of most recent Authorization to Operate (ATO):** The ATO applicable to NLPRP, titled "Source_LPR" was last issued on January 30, 2020, and expires on February 28, 2025. The DEASIL ATO was also issued January 30, 2020, but is due for renewal September 30, 2024. **If an ATO has not been completed, but is underway, provide status or expected completion date:**
X	**Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** A POAM for the Source-LPR system exists regarding the Deputy Attorney General Memorandum of March 1, 2023, and related to omission of certain privacy controls in the internal control tracking documentation for this system has been noted and is being corrected to ensure proper coverage by the monitoring system.

	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** Both the DEASIL and Source-LPR (NLPRP) security categorizations are based on the assessment of the potential impact that a loss of confidentiality, integrity, or availability would have on DEA operations, assets, individuals, other organizations, or the Nation. Security categories are used in conjunction with vulnerability and threat information in assessing the risk to DEA. Both the DEASIL and Source-LPR security categorizations are Moderate, an associated with both user information and system information. Security categorization standards for both DEASIL and Source1-LPR information provide an effective management and oversight of the DEASIL and Source-LPR systems.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** DEA monitors the information system on a continuous basis for changes to the information system or its operational environment, the information system security and privacy plan boundaries, or other conditions. DEA conducts security impact analyses of system associated changes, update of the information system's security plan and other relevant information system documentation, such as the system privacy plan, as appropriate, throughout the information system's lifecycle. However, an omission of certain privacy controls in the internal control tracking documentation for this system has been noted and is being corrected to ensure proper coverage by the monitoring system. DEA reports changes in the security or privacy status of the system to appropriate officials on a regular basis. Significant changes to the system require reauthorizations by the DEA Authorizing Official. Significant changes that effect the information system's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of PII are reviewed and assessed by the CPCLO, or a duly authorized official, prior to reauthorization by the Authorization Official. DEA ensures that the appropriate officials are made aware, in a timely manner, of information and the information system when it cannot be appropriately protected or secured, and that such is given a high priority for upgrade, replacement, or retirement.

X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** DEA has procedures that allow for the auditing of the creation, modification and use of user accounts at the keystroke level. The inputting of all information requests and alerts and the viewing of information received in response to requests and alerts is logged and auditable by DEA. Security personnel conduct quarterly audits relating to IT security as part of the standard operation and maintenance of the NLPRP. DEA security personnel also conduct Security and Privacy Assessment and Authorization (SPAA).
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** DEA authorized users must certify on a yearly basis that they have completed the annual security awareness training. A user guide is provided to new users, with the Rules of Behavior. A mandatory NLPRP training module is in development. A privacy module is included in that training package.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

The NLPRP has implemented various privacy and security controls, including administrative, technical, and physical measures, to minimize privacy risks and ensure compliance with the Constitution and applicable laws. These controls aim to reduce the risk of unauthorized access and disclosure and detect potential unauthorized access through regular auditing of role-based access.

Access controls are employed to reduce the risk of unauthorized access and disclosure. The NLPRP information is stored in a building with restricted access. Passwords, password protection identification features, and other system protection methods protect access to the system. Access to NLPRP information is granted only to authorized users and personnel who maintain the system. Moreover, the system automatically restricts user accounts after 30 days of inactivity and has other protection features. To further enhance security, NLPRP is developing a software token Multi Factor Authentication (MFA) system in collaboration with a commercial vendor, as described in Section 2 “Upcoming Updates to the NLPRP System.”

Administrative and technological controls secure information across both the NLPRP System and the DEASIL application to facilitate continuous oversight. Access to specific information within the NLPRP System and the DEASIL application is restricted based on user-assigned

roles. Security Administrators oversee system security logs and audit trails for both segments, while User Access Managers manage user accounts and access privileges.

Before allowing authorized users access to the system, all users must read and comply with NLPRP's Rules of Behavior, which include limitations to ensure privacy protection, receive system training, and periodically recertify for continued access. Annual security awareness training (which includes privacy awareness and Privacy Act training) is mandatory for DEA users.

Additional measures are taken to reduce the risk of unauthorized disclosure, data breaches, or receipt by unauthorized recipients include:

1. Limiting access to authorized users.

2. Requiring user input to access data.

3. Participating agencies must sign MOUs outlining program participation requirements, including recipient safeguards for appropriate use.

4. Establishing contracts with parties responsible for protecting and maintaining the program's security and functionality.

5. To guard against unauthorized disclosure, the information in the NLPRP system and the DEASIL application is safeguarded according to applicable laws, rules, and policies, including DEA's automated systems security, access, and anti-virus policies. The NLPRP System operates as a closed network and securely stores the information. Only authorized users with proper permissions can access LPR records stored in the NLPRP System via the DEASIL interface.

6. Authorized users submitting investigative requests or alerts on behalf of others must include identifying information of the person on whose behalf the request or alert is entered. Thus, all requests and alerts can be associated with the original requestor.

The NLPRP is protected in compliance with Department of Justice guidelines for Information Technology Security (DOJ 2640.2F) pertaining to both physical and environmental security. NLPRP computing equipment and electronic media are protected in accordance with the sensitivity of the information they are authorized to process, store, or transmit.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Information captured by LPR cameras, including images and data, transmitted to the NLPRP system become inaccessible to users within 90 days from the date of their collection if not included in a case file. The vast majority of NLPRP information is never specifically viewed

by a human being. Only images and data in the NLPRP system that are determined to be relevant to an investigation are accessed, downloaded, and stored in an investigative case file.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. ___X__ Yes.

LPR records determined to be relevant to an investigation and exported into an investigative case file is covered by JUSTICE/DEA-008, *Investigative Reporting and Filing System,* at 77 Fed. Reg. 21,808 (April 11, 2012). DEA is in the process of amending DEA-008 which will include updates reflecting the NLPRP.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

JUSTICE/DEA-008*, Investigative Reporting and Filing System, 77 Fed. Reg. 21,808 (April 11, 2012).* https://www.govinfo.gov/content/pkg/FR-2012-04-11/pdf/2012-8764.pdf

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the* collection, use, access, dissemination, and maintenance *of the information and how are those risks being mitigated?

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

a. Potential Threats Related to The Collection of the Information.

Privacy Risk: The NLPRP system may incorporate such large numbers of other governmental LPR network cameras and/or may acquire commercial LPR cameras system data in a large enough quantity in the future to effectively permit on-going tracking of individual's travels posing a risk to individual privacy.

Mitigation: This risk is mitigated. Currently, the only other federal government LPR system being incorporated in NLPRP is the camera data from the Customs and Border Protection (CBP) that is limited in scope. No commercially acquired LPR images are available to search in the NLPRP system. Although many state and local partner agencies have joined the NLPRP to aggregate the LPR network and enhance search capabilities, the scale of coverage is not extensive enough to enable comprehensive nationwide tracking surveillance considering the over 4 million miles of roads and streets in the country. The NLPRP encompasses a specific network of cameras, which are strategically deployed in specific locations, such as high-level drug trafficking corridors and on other public roadways. The number of cameras incorporated into the NLPRP remains limited, and their placement is determined by specific operational needs and priorities. The intention is to capture license plate data in areas where there is a particular focus on law enforcement and public safety, rather than achieving ubiquitous surveillance coverage.

Additionally, the NLPRP operates within the boundaries of legal and regulatory frameworks, as well as the Memoranda of Understanding or Agreement between DEA and participating agencies, ensuring that the use of LPR data is governed by applicable laws ,constitutional limitations and DEA LPR policy. Likewise, LPR data is shared through DEASIL, which a ROB that authorized users must read and acknowledge at least once a year. By acknowledging the ROB, users agree to abide by various rules, including the permissible uses of LPR data. Furthermore, the NLPRP system automatically renders information inaccessible within 90 days if it remains unviewed or is deemed irrelevant. This ensures data minimization and limits the retention period. The system also undergoes quarterly audits and assessments by the EPIC management to monitor compliance with policies and procedures, as well as to detect and investigate unauthorized access and use of data.

Privacy Risk: The NLPRP risks an over-collection of the PII of every license plate passing each LPR camera location, including a large number of images of travel of law-abiding drivers not relevant to criminal investigations.

Mitigation: This risk is partly mitigated. The NLPRP is carefully implemented and managed to minimize the impact on personal privacy, and to ensure compliance with the Constitution and applicable laws. The license plate images collected by the NLPRP are limited in scope to the plate and some surrounding environment but with no present automated capability as part of the NLPRP system to use facial recognition technology to identify occupants, nor any intent to deploy such technology in the future. Further, license plates are intended to be displayed in public view with little to no expectation of privacy. Although there is always some potential risk to privacy when the government creates of collection of a type of otherwise public information linked to particular individuals, the risk would be heightened if the government kept such information for extended periods and had such extensive coverage of the roadways with LPRs to permit tracking of vehicle's movements over that extended period of time. However, the NLPRP system keeps only 90 days' worth of LPR images and, as noted above, the numbers of cameras deployed does not provide sufficient coverage to permit real-time tracking nor piecing together a useful history of travels over time.

Privacy Risk: NLPRP's LPR cameras may misread a license plate due to a number of factors including weather conditions and damaged plates. Such misreads may lead to discrepancies

between the queried plate number and the results provided by the system causing misidentification of vehicles. This poses a risk to individual privacy.

Mitigation: This risk is partly mitigated. Generally, the nature and quality of information can present risks to privacy, particularly when the individual is not the source of the information obtained about him/her. In this case, the information captured in photographs by LPR cameras is not subject to the inaccuracies of information captured by human observation and transmittal. OCR technology provides license plate number information as determined by its algorithm or, if obscured by weather, plate damage or obstruction, the system will provide a percentage-based degree of confidence indicating how closely the recognized license plate matches the license plate number of interest, as determined by the OCR technology. Importantly, the photographs themselves are available for human review and confirmation. Further, when users receive information responsive to an alert, they are notified that LPR data cannot be used as the only reason for law enforcement action.

NLPRP data is accessible through DEASIL, which contains Rules of Behavior (ROB) for using the system. Authorized users must read and acknowledge the ROB and agree to various requirements. NLPRP ROB requires authorized users to visually verify that the license plate photographed is the license plate of interest to ensure an accurate match and reduce the risk of errors. Essentially, the system provides only a percentage degree of confidence, a positive search result must be reviewed by a human and the search result cannot be used as the only reason for law enforcement action. Violations of these rules may result in temporary suspension of system access, permanent revocation, or civil and/or criminal penalties for both the user and the user's agency.

b. Potential Threats Related to Use and Maintenance of the Information

Privacy Risk: There is a risk of LPR information being used for an unauthorized purpose, including unwarranted surveillance or other actions that could implicate violation of constitutionally protected rights under the 1st and 4th Amendment.

Mitigation: This risk is mitigated. The NLPRP's ROB authorize users to only query and retain LPR records connected to a criminal investigation or related to missing person cases. Only users who have an investigative need and reasonable articulable suspicion that a particular license plate is involved in criminal activity or a missing person situation or who have a need to conduct an investigative request in furtherance of lawful purposes associated with a traffic stop may conduct an investigative request or set up an alert. User activities are monitored through quarterly audits to ensure that the system is used appropriately and use of LPR data is limited to legitimate law enforcement purposes. Also, information that is collected and maintained on the NLPRP system but is not accessed or has been viewed but deemed irrelevant by the User, will become inaccessible and purged from the system within 90 days from its collection. Additionally, all DEA personnel with access to DEA's information technology, including the NLPRP, are required to complete annual security awareness training, to agree to information technology rules of behavior, and to be subject to discipline for violations of rules of behavior. Non-DEA users must agree to abide by NLPRP rules of behavior. Finally, DEA conducts regular audits and assessments to monitor compliance with these policies and

procedures and to detect unauthorized access and use of data. Any such incidents are investigated, and appropriate action is taken, including revoking system access privileges and/or facing severe civil or criminal penalties, if applicable.

Privacy Risk: There is always some risk present that system information, either at rest or in transmission, is susceptible to compromise without sufficient technical, and administrative privacy and security controls to protecting from technological/cyber breach (e.g., Hacking) or from an "Insider Threat" actions resulting in a breach.

Mitigation: This risk is mitigated. The NLPRP is governed by DOJ Order 0904-Cybersecurity Program and the DOJ cybersecurity standards (derived from NIST 800-53 Rev. 5[9]) for applying security controls and safeguards to information systems. The NLPRP system employs a multi-layered defense-in-depth security approach. Through a combination of perimeter and internal hardware and software security safeguard mechanisms, DEA ensures security controls protect organizational objectives. The security defenses include layered perimeter security safeguards and internal host-based security protection mechanisms. The perimeter architecture consists of perimeter firewalls, perimeter routers, Next-Gen firewalls, and intrusion detection/prevention systems. Internal security protection mechanisms include endpoint protection, host-based malware and proactive threat protection, database encryption, and advanced system and event logging. In addition, DEA manages user identities in accordance with Homeland Security Presidential Directive-12 Personal Identity Verification (PIV) compliance, and DEA's Identity Credential and Access Management policy. This ensures that only approved and vetted users are able to access the DEA network. The NLPRP also enforces secure configuration management to ensure the system adheres to security controls appropriate for its risk level. The NLPRP system follows the established DOJ and DEA continuous monitoring strategy, including utilizing Security Information and Event Manager monitoring systems. Additionally, consistent with NIST security controls, transmissions of DEA non-public data occur only through secure methods, e.g., Virtual Private Networks (VPN), Secure File Transfer Protocol (SFTP), Secure Sockets Layer (SSL), or other FIPS 140-2 approved encryption methods. These encryption methods ensure that data cannot be viewed in plain text by unauthorized users.

As noted at Section 6.2, to further enhance security, NLPRP is developing a software token Multi-Factor Authentication (MFA) system in collaboration with a commercial vendor, as described in Section 2 "Upcoming Updates to the NLPRP System."

Privacy Risk: DEA may not appropriately monitor, test and evaluate NLPRP privacy and security controls to safeguard PII and may inadequately perform auditing of system use to ensure compliance with security and privacy standards.

Mitigation: This risk is partially mitigated. A system of monitoring, testing and evaluation does exist on NLPRP (See Section 6.1, 5th topic). Although there has been a shortcoming in the internal control tracking documentation that improperly omitted certain privacy controls, those controls nonetheless were recognized as necessary and prompted the completion of this

[9] See https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

Privacy Impact Assessment. A POAM has been created regarding the internal documentation issue to ensure that all privacy controls are properly included into the monitoring system referenced above. Further, security personnel conduct quarterly audits relating to IT security as part of the standard operation and maintenance of the NLPRP. DEA security personnel also conduct Certification and Authorization processes.

Privacy Risk: Retaining LPR records for extended periods poses significant privacy risks. Prolonged retention of this data increases the likelihood of unauthorized dissemination or misuse, potentially leading to abuse or the targeting of individuals without just cause. There is also the risk of this information being improperly shared or used in ways that extend beyond the original law enforcement purposes, potentially infringing on individuals' privacy rights.

Mitigation: Such risks are mitigated by this system. The NLPRP does not keep its information indefinitely nor does DEA share NLPR records for reasons incompatible with the purposes for which the information was appropriately collected. The NLPRP System is designed for license plate reader images to be retained for a limited duration of 90 days. To retain a LPR record beyond 90 days, a requestor would need to download the image during the 90-day window to a relevant investigative case file. Further, NLPRP data is used and shared in a manner consistent with this privacy impact assessment and, when applicable, the Privacy Act, the routine uses in the SORN.

c. Potential Threats Related to Dissemination of the Information

Privacy Risk: There is a risk of unauthorized disclosure of LPR data outside DEA or receipt of LPR data by unauthorized recipients.

Mitigation: This risk is partially mitigated through various measures. Disclosure of LPR data outside DEA must comply with DEA information sharing policy and Privacy Act requirements, potentially including routine use limitations for disclosures outside DOJ. All users of the NLPRP system are required to read and comply with the ROB established by the NLPRP. Additionally, access to the NLPRP system is limited to authorized personnel with an official need-to-know, so that only those who require access for their job responsibilities can obtain it. All DEA personnel with access to NLPRP system must have an official need for accessing the NLPRP system. DEA users are also required to complete annual security awareness training. Access to the NLPRP system by non-DEA personnel is also restricted to vetted and trained authorized users. To gain access to the NLPRP system through DEASIL, Non-DEA applicants are required to undergo a background screening and provide personally identifying information, along with details about their employing agency. Additionally, the applicant's supervisor and the security coordinator from their agency must grant authorization, ensuring that the individual requesting access has a legitimate need for accessing the system to carry out their official duties. NLPRP data can only be disseminated to authorized law enforcement personnel with proper authority, for authorized purposes, and consistent with standing information sharing agreements or as otherwise authorized by the DEA. These limitations are enforced in different ways for NLPRP system users versus non-users. For system users, only authorized users can access and download LPR records, and such accesses and downloads are audited. For non-users, however, once the data is downloaded from the system, there is no way to conduct audits to ensure the data is disseminated or used

appropriately. Appropriate information handling and use requirements are included in the MOUs between DEA and the state, local, tribal, territorial information recipient agencies and are enforced by those recipient agencies. All investigative requests and alerts must contain authorized user's identifying information and the person on whose behalf the request or alert is entered, if applicable. This ensures that all requests and alerts can be associated with the original requestor and helps prevent unauthorized access or use of the information. Finally, all law enforcement agencies involved in the network have information sharing agreements with the DEA, detailing the parameters for using and sharing the LPR information. DEA and its law enforcement partners have also instituted NLPRP policies and procedures to protect individual privacy and civil liberties.

APPENDIX

EXAMPLES OF OPERATIVE NLPRP MEMORANDA OF UNDERSTANDING

1. Template of Standard LPR Sharing MOU

National License Plate Reader Program – Data Sharing

MEMORANDUM OF UNDERSTANDING

between the

[Agency Name, City, State]

and the

U.S. Department of Justice, Drug Enforcement Administration

regarding

License Plate Reader Information

1. PARTIES

   The Parties to this Memorandum of Understanding (MOU) are the ***[Agency Name]*** and the U.S. Department of Justice, Drug Enforcement Administration (DEA), collectively "the Parties."

2. PURPOSE

   The purpose of this MOU is to support the missions of the ***[Agency Name]*** and DEA by 1) establishing the terms and conditions for sharing license plate reader (LPR) information and 2) establishing the terms and conditions for the Parties' use and further dissemination of LPR information.

3. DEFINITIONS

   3.1 "License Plate Readers" (LPRs) are devices that capture LPR information regarding vehicles in the vicinity of the LPR.

   3.2 "LPR information" is information obtained by an LPR. Typically, it includes images of vehicles and license plates, the location at which the vehicle/license plate was photographed, the date and time the images were captured, and identifying information for the LPR itself. It may also include images of the drivers and occupants of the vehicles and passersby.

   3.3 "The National License Plate Reader Network" (the NLPRN) is a network created and managed by DEA that contains LPR information obtained from LPRs belonging to federal, state, local and tribal law enforcement officials and that is accessed by federal, state, local and tribal law enforcement officials. The network allows law enforcement officials to search LPR information contained within the network.

4. AUTHORITIES

1 of 5

National License Plate Reader Program – Data Sharing

4.1 The ***[Agency Name]*** is authorized to enter into this MOU pursuant to ***[Enter Specific Authority Here (e.g. state law, statute, act, policy, ordinance, etc.)]***.

4.2 DEA is authorized to enter into this MOU pursuant to the Comprehensive Drug Abuse Prevention and Control Act of 1970, as amended, 21 U.S.C. § 801 *et seq.* The specific authority for DEA to enter into cooperative agreements for the exchange of information between governmental officials concerning the use and abuse of controlled substances is 21 U.S.C. § 873.

5. SHARING AND USE OF LPR INFORMATION

5.1 The Sharing of LPR Information

5.1.1 The ***[Agency Name]*** shall provide DEA with LPR information in near real-time. The information shall be transmitted via a method agreed to by both parties, which may include, but is not limited to, VPN, secure Internet connection or approved direct server feed.

5.1.2 The ***[Agency Name]*** if capable, shall tag the LPR information it provides to DEA so that subsequent recipients can ascertain from which agency it originated. If ***[Agency Name]*** is not capable of tagging the LPR information, DEA will tag the LPR information to indicate which agency it came from.

5.1.3 Employees whom ***[Agency Name]*** sponsors, who apply for access to the NLPRN, and whom DEA authorizes shall be permitted to access LPR information in the NLPRN.

5.1.4 DEA and ***[Agency Name]*** shall provide each other with the name of its point of contact regarding this MOU and update the point of contact if he/she changes.

5.2 The Use of LPR Information

5.2.1 The ***[Agency Name]***'s use of LPR information from the NLPRN obtained pursuant to this MOU shall be in accordance with applicable law, this MOU, and any Rules of Behavior and training required prior to use of the NLPRN.

5.2.2 The ***[Agency Name]***'s users shall access LPR information in the NLPRN only for the investigation of drug trafficking offenses, money laundering, other crimes, Amber alerts, and silver alerts, and in furtherance of the mission of a traffic stop.

5.2.3 The ***[Agency Name]***'s users shall not take any operational action based solely on LPR information from the NLPRN.

National License Plate Reader Program – Data Sharing

5.2.4 The ***[Agency Name]*** will provide to DEA a quarterly consolidated statistical report describing significant enforcement activities resulting from the utilization of the LPR system. At a minimum, the report will include arrests, drug seizures, and asset seizures, but may be expanded to include other significant enforcement statistical measures. The report will be submitted via email to LPR@usdoj.gov no later than the last calendar day of the fiscal quarter.

5.3 The Parties are authorized to redisseminate for operational purposes LPR information obtained pursuant to this MOU only in accordance with applicable law, this MOU, and any Rules of Behavior and training required prior to use of the NLPRN.

6. FEDERAL AND STATE LAW OPEN RECORDS AND FREEDOM OF INFORMATION REQUESTS

When ***[Agency Name]*** receives open records and freedom of information requests for LPR information, ***[Agency Name]*** shall notify DEA and give DEA an opportunity to review the request to determine whether it has any equities in the requested information. If DEA determines that it has equities in the information, and that the information should not be released, ***[Agency Name]*** will protect the information to the extent possible consistent with state law.

7. INFORMATION SECURITY, RETENTION, AND INTEGRITY

7.1 The Parties agree to maintain administrative, technical, and physical safeguards appropriate to the sensitivity of, and designed to appropriately protect, the LPR information shared under this MOU against loss, theft, and misuse and unauthorized access, disclosure, copying, use, modification, storage, and deletion in accordance with the Federal Information Security Modernization Act, any similar, applicable state statute, and any applicable Privacy Act system of records notice. These safeguards must include audit capabilities that identify the LPR information the Parties disseminated pursuant to section 5.3 of this MOU and a point of contact within the entity that received the LPR information.

7.2 LPR information received pursuant to this MOU in the NLPRN will remain available for up to, but no longer than, a 90-day period. If relevant to a DEA investigation or case, LPR information received by DEA pursuant to this MOU may be moved to and maintained in a separate system that is governed by an alternate destruction schedule, in which case that alternate destruction schedule will be followed. In the event that LPR information is maintained in a federal Privacy Act system or systems of records, or a state equivalent of a federal Privacy Act system or systems of records, the information shall be

National License Plate Reader Program – Data Sharing

maintained, shared, and used in accordance with the applicable system of records notice(s) and sections 5.2 and 6 of this MOU.

7.3 Each party shall contact the other party's point of contact to obtain the other party's incident-reporting policy. When there has been or may have been loss, theft, or misuse or unauthorized access, disclosure, copying, use, modification, storage, or deletion of LPR information received pursuant to this MOU, the party discovering the unauthorized activity shall promptly report to, and consult with, the other party in accordance with the reporting party's incident-reporting policy.

8. COSTS

This MOU is not an obligation or commitments of funds, nor a basis for transfer of funds. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to the party's budgetary processes and the availability of funds and resources pursuant to applicable laws, regulations, and policies. The Parties expressly acknowledge that this in no way implies an appropriation of funds for such expenditures.

9. SEVERABILITY

Nothing in this MOU is intended to conflict with applicable federal or state law, or with the policy of any party. If a provision of this MOU is inconsistent with applicable federal or state law, or with a party's policy, then the party shall immediately so advise the other party, and the Parties shall determine whether the remaining provisions of this MOU shall continue in effect.

10. EFFECT ON OTHER AUTHORITIES

Nothing in this MOU is intended to restrict the authority of any party to act as permitted by law, or to restrict any party from administering or enforcing any law.

11. EFFECTIVE DATE

This MOU will become effective when signed by the representatives of all of the Parties.

12. MODIFICATION

The Parties may jointly agree in writing to modify this MOU.

13. TERMINATION

Any party may terminate this MOU by giving thirty (30) days' written notice to the other party. In the event of termination, all provisions regarding the LPR information obtained pursuant to this MOU shall remain in effect.

National License Plate Reader Program – Data Sharing

14. DURATION AND EFFECT OF THE MOU

The Parties intend to begin cooperation under this MOU upon signature by both Parties. Cooperation is intended to continue for five (5) years unless amended, in writing, by signature of the Parties or terminated, in writing, by either party upon thirty (30) days' written notice to the other party. The Parties agree to review the MOU annually to assess its effectiveness.

15. NO PRIVATE RIGHTS CREATED

This MOU does not create any right or benefit, substantive or procedural, enforceable in law or in equity, against the United States or any state, against any department, agency, officer, or employee of the United States or any state, against any entity, or against any other person.

For the *[Agency Name]*:

_____ Date:_____
(Signature)

(Print/typed name and title)

For DEA:

_____ Date:_____
[Name]
[Position]
Drug Enforcement Administration

2. Template of LPR Sharing MOU for Regional Hubs

National License Plate Reader Program – Data Sharing and Hub

MEMORANDUM OF UNDERSTANDING

between the

[Agency Name, City, State]

and the

U.S. Department of Justice, Drug Enforcement Administration

regarding

License Plate Reader Information

1. PARTIES

   The Parties to this Memorandum of Understanding (MOU) are the ***[Agency Name]*** and the U.S. Department of Justice, Drug Enforcement Administration (DEA), collectively "the Parties." The ***[Agency Name]*** is a law enforcement agency within the State of ***[State Name]***, and has established written agreements with several state and local law enforcement agencies that contribute license plate reader data, hereinafter "Contributing Agencies," that include but are not limited to the entities listed in the appendix to this agreement.

2. PURPOSE

   The purpose of this MOU is to support the missions of the ***[Agency Name]*** and DEA by 1) establishing the terms and conditions for sharing license plate reader (LPR) information, and 2) establishing the terms and conditions for the Parties' use and further dissemination of LPR information.

3. DEFINITIONS

   3.1 "License Plate Readers" (LPRs) are devices that capture LPR information regarding vehicles in the vicinity of the LPR.

   3.2 "LPR information" is information obtained by an LPR. Typically, it includes images of vehicles and license plates, the location at which the vehicle/license plate was photographed, the date and time the images were captured, and identifying information for the LPR itself. It may also include images of the drivers and occupants of the vehicles and passersby.

   3.3 "The National License Plate Reader Network" (the NLPRN) is a network created and managed by DEA that contains LPR information obtained from LPRs belonging to federal, state, local and tribal law enforcement officials and that is accessed by federal, state, local and tribal law enforcement

officials. The network allows law enforcement officials to search LPR information contained within the network.

4. AUTHORITIES

4.1 ***[Agency Name]*** is authorized to enter into this MOU pursuant to ***[Enter Specific Authority Here (e.g. state law, statute, act, policy, ordinance, etc.].*** The Parties intend for ***[Agency Name]*** to enter into sub-agreements with state and local law enforcement agencies within the State of ***[State Name]*** (Contributing Agencies) to contribute LPR information to the NLPRN consistent with this MOU, pursuant to this same authority.

4.2 DEA is authorized to enter into this MOU pursuant to the Comprehensive Drug Abuse Prevention and Control Act of 1970, as amended, 21 U.S.C. § 801 *et seq.* The specific authority for DEA to enter into cooperative agreements for the exchange of information between governmental officials concerning the use and abuse of controlled substances is 21 U.S.C. § 873.

5. SHARING AND USE OF LPR INFORMATION

5.1 The Sharing of LPR Information

5.1.1 [***Agency Name***] shall enable Contributing Agencies to provide DEA with LPR information in near real-time. The information shall be transmitted via a method agreed to by both parties, which may include, but is not limited to, VPN, secure Internet connection or approved direct server feed.

5.1.2 [***Agency Name***] will notify Contributing Agencies that they shall, if capable, tag the LPR information provided to DEA so that subsequent recipients can ascertain from which agency it originated. If Contributing Agencies are not capable of tagging the LPR information, DEA will tag the LPR information to indicate which agency it came from.

5.1.3 Employees whom [***Agency Name***] and/or Contributing Agencies sponsor, who apply for access to the NLPRN, and whom DEA authorizes shall be permitted to access LPR information in the NLPRN.

5.1.4 DEA and [***Agency Name***] shall provide each other with the name of its point of contact regarding this MOU and update the point of contact if he/she changes.

5.2 The Use of LPR Information

5.2.1 The written agreements between [***Agency Name***] and the

Contributing Agencies state that the Contributing Agencies will agree that [***Agency Name***] shall provide notification to Contributing Agencies that their use of LPR information from the [***Agency Name***] obtained pursuant to this MOU and any sub-agreement shall be in accordance with applicable law, this MOU, ***[Enter any other applicable citations (e.g. CJIS agreements, agency user agreements, etc.]***, and any Rules of Behavior and training required prior to use of the NLPRN.

5.2.2 ***[Agency Name]*** shall provide notification to Contributing Agencies that Contributing Agencies' users shall access LPR information in the NLPRN only for the investigation of drug trafficking offenses, money laundering, other crimes, Amber alerts, and in furtherance of the mission of a traffic stop.

5.2.3 ***[Agency Name]*** shall provide notification to Contributing Agencies that Contributing Agencies' users shall not take any operational action based solely on LPR information from the NLPRN.

5.2.4 The ***[Agency Name]*** will provide to DEA a quarterly consolidated statistical report describing significant enforcement activities resulting from the utilization of the LPR system. At a minimum, the report will include arrests, drug seizures, and asset seizures, but may be expanded to include other significant enforcement statistical measures. The report will be submitted via email to LPR@usdoj.gov no later than the last calendar day of the fiscal quarter.

5.3 The Parties and Contributing Agencies are authorized to redisseminate for operational purposes LPR information obtained pursuant to this MOU only in accordance with applicable law, this MOU, and any Rules of Behavior and training required prior to use of the NLPRN.

6. FEDERAL AND STATE LAW OPEN RECORDS AND FREEDOM OF INFORMATION REQUESTS

When ***[Agency Name]*** or a Contributing Agency receives open records and freedom of information requests for LPR information, ***[Agency Name]*** or the Contributing Agency shall notify DEA and give DEA an opportunity to review the request to determine whether it has any equities in the requested information. If DEA determines that it has equities in the information, and that the information should not be released, ***[Agency Name]*** or the Contributing Agency will protect the information to the extent possible consistent with applicable state law.

7. INFORMATION SECURITY, RETENTION, AND INTEGRITY

7.1 The Parties agree to maintain administrative, technical, and physical safeguards appropriate to the sensitivity of, and designed to appropriately protect, the LPR information shared under this MOU against loss, theft, and misuse and unauthorized access, disclosure, copying, use, modification, storage, and deletion in accordance with the Federal Information Security Modernization Act, any similar, applicable state statute, and any applicable Privacy Act system of records notice. These safeguards must include audit capabilities that identify the LPR information the Parties disseminated pursuant to section 5.3 of this MOU and a point of contact within the entity that received the LPR information.

7.2 LPR information received pursuant to this MOU in the NLPRN will remain available for up to, but no longer than a 90-day period. If relevant to a DEA investigation or case, LPR information received by DEA pursuant to this MOU may be moved to and maintained in a separate system that is governed by an alternate destruction schedule, in which case that alternate destruction schedule will be followed. The written agreements between ***[Agency Name]*** and the Contributing Agencies state that the Contributing Agencies will agree that, in the event that LPR information is maintained in a federal Privacy Act system or systems of records, or a state equivalent of a federal Privacy Act system or systems of records, the information shall be maintained, shared, and used in accordance with the applicable system of records notice(s) and sections 5.2 and 6 of this MOU.

7.3 Each party shall contact the other party's point of contact to obtain the other party's incident-reporting policy. When there has been or may have been loss, theft, or misuse or unauthorized access, disclosure, copying, use, modification, storage, or deletion of LPR information received pursuant to this MOU, the party discovering the unauthorized activity shall promptly report to, and consult with, the other party in accordance with the reporting party's incident-reporting policy.

8. COSTS

This MOU is not an obligation or commitments of funds, nor a basis for transfer of funds. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to the party's budgetary processes and the availability of funds and resources pursuant to applicable laws, regulations, and policies. The Parties expressly acknowledge that this in no way implies an appropriation of funds for such expenditures.

9. SEVERABILITY

Nothing in this MOU is intended to conflict with applicable federal or state law, or with the policy of any party. If a provision of this MOU is inconsistent with applicable federal or state law, or with a party's policy, then the party shall immediately so advise the other party, and the Parties shall determine whether the

remaining provisions of this MOU shall continue in effect.

10. EFFECT ON OTHER AUTHORITIES

Nothing in this MOU is intended to restrict the authority of any party to act as permitted by law, or to restrict any party from administering or enforcing any law.

11. EFFECTIVE DATE

This MOU will become effective when signed by the representatives of all of the Parties.

12. MODIFICATION

The Parties may jointly agree in writing to modify this MOU.

13. TERMINATION

Any party may terminate this MOU by giving thirty (30) days' written notice to the other party. In the event of termination, all provisions regarding the LPR information obtained pursuant to this MOU shall remain in effect.

14. DURATION AND EFFECT OF THE MOU

The Parties intend to begin cooperation under this MOU upon signature by both Parties. Cooperation is intended to continue for five (5) years unless amended, in writing, by signature of the Parties or terminated, in writing, by either party upon thirty (30) days' written notice to the other party. The Parties agree to review the MOU annually to assess its effectiveness.

15. NO PRIVATE RIGHTS CREATED

This MOU does not create any right or benefit, substantive or procedural, enforceable in law or in equity, against the United States or any state, against any department, agency, officer, or employee of the United States or any state, against any entity, or against any other person.

National License Plate Reader Program – Data Sharing and Hub

For *[Agency Name]*:

_____ Date:_____
(Signature)

_____
(Print/typed name and title)

For DEA:

_____ Date:_____
[Name]
[Position]
Drug Enforcement Administration

National License Plate Reader Program – Data Sharing and Hub

Appendix A – Contributing Agencies

[Contributing Agency Name 1]
[Contributing Agency Name 2]
[Contributing Agency Name 3]
[Contributing Agency Name 4]
[Contributing Agency Name 5]