Drug Enforcement Administration

Privacy Impact Assessment
for the
National License Plate Reader Program (NLPRP)

Issued by:
David J. Mudd
Senior Component Official for Privacy
Drug Enforcement Administration

Approved by: Peter A. Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: April, 17, 2019

(May 2015 DOJ PIA Template)

Points of Contact and Signatures

COMPONENT PRIVACY POINT OF CONTACT (POC) Name: Mary C. Donovan Office: SIBC Phone: 202-307-1257 Bldg./Room Number: E-3219 Email: Mary.C.Donovan@usdoj.gov	**PIA AUTHOR** (if different from POC) Name: Paul Knierim Office: Acting Chief of Intelligence Phone: 202-353-7858 Bldg./Room Number: W-11024 Email: Paul.E.Knierim@usdoj.gov
SECURITY REVIEW OFFICIAL (Component CIO/OBD Executive Officer/OCIO Staff Director/JMD Staff Director) Name: Preston L. Grubbs Office: Operational Support Division Phone: 202-307-4730 Bldg./Room Number: W-12142-A Email: Preston.L.Grubbs@usdoj.gov Signature: _____ Date signed: _____	**SENIOR COMPONENT OFFICIAL FOR PRIVACY** (if designated; otherwise POC) Name: David J. Mudd Office: Office of Chief Counsel Phone: 202-598-8707 Bldg./Room Number: E-12161 Email: David.J.Mudd@usdoj.gov Signature: _____ Date signed: _____

DOJ PIA APPROVING OFFICIAL
Peter A. Winn
Acting Chief Privacy and Civil Liberties Officer,
Assistant Deputy Attorney General
U.S. Department of Justice
(202) 514-2101

Signature: _____

Date signed: _____

THIS PAGE IS FOR INTERNAL ROUTING PURPOSES AND DOCUMENTATION OF APPROVALS. UPON FINAL APPROVAL, COMPONENTS SHOULD REMOVE THIS PAGE PRIOR TO PUBLICATION OF THE PIA

EXECUTIVE SUMMARY

The Drug Enforcement Administration's (DEA) National License Plate Reader Program (NLPRP) is a law enforcement tool developed and used to meet threats raised by drug trafficking, money laundering and other criminal activities occurring on high-level drug and money trafficking corridors and other public roadways throughout the United States.

DEA is conducting this Privacy Impact Assessment to provide the public notice of the NLPRP and to assure the public that the NLPRP is properly implemented and carefully managed to minimize the impact on personal privacy and to ensure compliance with the Constitution and applicable laws.

Section 1: Description of the Information System

Provide a non-technical overall description of the system that addresses:

(a) the purpose that the records and/or system are designed to serve;

The mission statement of the NLPRP is: "The Drug Enforcement Administration's (DEA) National License Plate Reader Program (NLPRP) 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. Given its unique capabilities, secure and vetted access to this tool is also shared with state, local and other federal law enforcement partners nationwide. The goal is to assist with criminal 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. DEA, and its law enforcement partners, have instituted NLPRP policies and procedures that protect individual privacy and civil liberties."

A large portion of the illegal substances introduced into the United States for distribution, and the majority of drug proceeds derived in the United States, are transported over land routes in vehicles using hidden/concealed compartments. The NLPRP uses license plate reader (LPR) technology to collect images of vehicle license plates for law enforcement to address threats raised by drug trafficking, money laundering, and other criminal activity on high-level drug and money trafficking corridors and other public roadways throughout the United States. Vehicle license plate numbers are frequently the only identifying information available to law enforcement during criminal investigations. Similarly, law enforcement agencies routinely associate vehicle license plate numbers with specific criminal activities. The NLPRP allows authorized users to conduct queries of recent historical location information for vehicles known to be associated with criminal activity or a missing person and to set up alerts to be notified when a vehicle known to be associated with criminal activity or a missing person is recognized by a LPR connected to the NLPRP system. In addition, the NLPRP allows authorized users to conduct queries of recent historical location information during a traffic stop when that query is lawful and done in furtherance of the traffic stop mission.

(b) the way the system operates to achieve the purpose(s);

The NLPRP is an investigative tool that uses LPRs to provide law enforcement personnel with

information about vehicle license plates to assist in investigating narcotics trafficking, bulk cash smuggling, other criminal offenses, and missing person cases and in support of the traffic stop mission. An LPR is a system consisting of a high-speed camera or cameras and related equipment, mounted on vehicles or in fixed locations. Cameras in fixed locations are stationary, and are used only on public roadways, or elsewhere with the permission of a property owner. Mobile readers are utilized only on official law enforcement vehicles or platforms.

The cameras automatically photograph license plates that come into visual range of the cameras. Once a photograph of a license plate is taken, the system automatically scans that image using Optical Character Recognition (OCR) technology to identify, as best as possible, the license plate number and, in some cases, the state of registration. The photographs sometimes also capture other portions of the vehicle or an overall image of the vehicle, the vehicle's make and model, and/or the environment surrounding the vehicle, which may include drivers, passengers, passersby, and/or other license plates. The system documents 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.

The NLPRP is a network of LPR equipment owned by DEA, other federal agencies, and state, local, and tribal police departments. All law enforcement agencies involved have Memorandums of Understanding with DEA detailing the parameters for use and sharing of the LPR information.

As described in more detail in Section 1(c) below, the NLPRP allows authorized users to 1) make investigative requests to determine whether a license plate of interest has been recognized by an LPR in the system within the previous 90 days, 2) set up an alert for a license plate of interest so that the user will be notified if the license plate is recognized by a LPR in the system within the next 30 days, and 3) conduct deconfliction to determine whether a particular license plate is also of interest in a different investigation. If an investigative request is made or an alert is set up and the license plate of interest has been or is recognized within the relevant timeframe, the user will be given access to the photographs and associated data obtained during that sighting or sightings.

(c) the type of information collected, maintained, used, or disseminated by the system;

The LPR cameras automatically photograph front and/or rear license plates that come into visual range of the cameras. Once a photograph of a license plate is taken, the system uses OCR technology to identify, as best as possible, the license plate number and, in some cases, the state of registration. Depending on the site and camera field of view, the photographs sometimes also capture other portions of the vehicle, including images of interior portions of the vehicle visible through a vehicle window, an overall image of the vehicle, the vehicle's make and model, and/or the environment surrounding the vehicle, which may include drivers, passengers, passersby, and/or other vehicles and license plates. The system documents 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. This information is maintained in the NLPRP system for 90 days from the date it is captured before it is unavailable to users and deleted from the system.

An authorized user may conduct investigative requests, set up alerts, or conduct deconfliction.

An investigative request allows a user to determine whether a license plate of interest has been recognized by a LPR in the system within the previous 90 days. In order to make an investigative request, the user must enter the following information: 1) the full or partial license plate number or container number (a reference number assigned to a freight container) of interest;[1] 2) the "match type" required for data to be responsive; 3) the maximum number of results requested, with options ranging from 100 to all responsive data; 4) the user's reason for conducting the request; 5) the agency and case number associated with the request; and 6) whether the user is making the request on behalf of himself or herself or another person, whose name and agency must be identified.

The available "match types" (item #2 above) include "exact," "contains," "no read," and "soundex." For a match to be "exact," the OCR read of the license plate must be exactly the characters of the license plate number entered by the user, no more or less. A "contains" search allows responsive license plate numbers to have additional characters before and/or after the characters entered by the user. A "no read" search allows a user to receive data relating to information captured when no characters were able to be read by the OCR technology. (This "no read" functionality will be removed for most users by approximately mid-May 2019. It will remain available thereafter only for administrative users.) A "soundex" search uses set rules to provide data that is similar to the license plate number of interest. For example, if the license plate of interest was "ABC L23," a "soundex" search may include the license plate number "ABC 123."

In addition, when making an investigative request, the user may enter the following information: 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).

Once the investigative request is submitted, the user will receive images and data that is responsive to the entries made by the user. The response may include, for each vehicle recognized with a license plate number that fits the criteria entered, the following information: 1) the degree of confidence, expressed in a percentage, that the license plate number recognized is a match with the license plate number of interest; 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; 4) sighting state; 5) sighting location; 6) roadway name, including the lane of the roadway; 7) direction of travel; 8) date(s) and time(s) recognized; 9) an image or images of the license plate, vehicle, and/or surrounding environment; and 10) identification name/number of the LPR camera. A user can conduct an interval search relating to a sighting of interest. An interval search allows a user to look at all images and data obtained from the same sighting location for up to 30 minutes before and 30 minutes after the sighting of interest.

[1] In the remainder of the document, for simplicity, the phrase "license plate number" is used to refer to license plate numbers and container numbers.

In exigent circumstances (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) and with the authorization of a Senior Executive Service-level supervisor, a limited number of authorized 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.

An authorized user is also able to set up alerts for license plates of interest. When an alert is set up for a license plate of interest, the user will be notified if the license plate is recognized by a LPR 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 himself or herself or 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 information of his or her choosing.

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.

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 should not be the basis for taking action. 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 recipient may also receive information regarding the nearest law enforcement agency point of contact.

There are two possible ways to conduct deconfliction, "alert deconfliction," which occurs through the DEA Special Intelligence Link (DEASIL), and "investigative deconfliction," which occurs in a separate DEA system, the Deconfliction and Information Coordination Endeavor (DICE). All DEASIL users automatically conduct "alert deconfliction" through DEASIL with each investigative request and each set-up of an alert. In DEASIL, "alert deconfliction" means that if more than one user sets an active alert on a specific target license plate number, or if a user conducts an investigative request on a license plate for which a different user has an existing alert, both users will receive an email "overlap" notification, generated automatically by the DEASIL system. This email will contain the name, agency and contact information for each user so they can make contact and deconflict investigations if so desired. No investigative information is disseminated via the automatic notification.

Non-DEA users can also conduct "investigative deconfliction" requests in DICE system. To do so, a user enters the license plate number of interest, the associated case number, and the user's name and contact information and the license plate state, if known. DICE checks license plate numbers that have previously been entered into DICE, and if two users have entered matching information on separate inquiries, each user will receive a conflict notification, including the name, agency and contact information for the other user. This aspect of the "investigative deconfliction" request in DICE does not involve the NLPRP. When a user conducts "investigative deconfliction" in DICE, DICE also queries the NLPRP database, and provides the user with basic historical sighting information, including the date(s), time(s), and location(s) of sightings within the prior 90 days. (The interconnection between the NLPRP and DICE will be discontinued in the near future.)

(d) who has access to information in the system;

Individuals who may access the NLPRP include law enforcement officers (LEOs) and non-LEOs, as specified below. LEOs include law enforcement officers who are employed by DEA and at federal, state, local, and tribal law enforcement agencies. Non-LEOs include intelligence analysts, dispatchers, and government attorneys working on criminal investigations. Users seeking access to the NLPRP who are not federal LEOs must be vetted by the El Paso Intelligence Center (EPIC) before being permitted to access the NLPRP. Each user must obtain a unique username and password and choose security challenge questions to assist in password recovery.

Authorized users may access information on their own behalves or on the behalf of personnel from law enforcement agencies and certain quasi-law enforcement agencies. 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.

DEA users access NLPRP through DEASIL. Non-DEA users access the NLPRP through DICE or DEASIL. Additional details on the interconnection between NLPRP, DICE, and DEASIL are given below in Section 1(g).

Access to specific information within the DEASIL LPR application is restricted by user-assigned roles, which include Regular User, Maintenance User, System Administrator, Security Administrator, and User Access Manager. Regular Users may conduct investigative requests and alerts, as described above. Regular Users may have membership in specific agency and law enforcement groups. These "groups" can make standard distribution lists comprised of some or all of the group's members for specific alert or investigative request responses, instead of adding each individual member for distribution of responsive information.

Maintenance Users have IT-related access for system management and maintenance. System Administrators, Security Administrators, and User Access Managers 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 database. The System Administrators are responsible for the maintenance and operation of 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.

(e) how information in the system is retrieved by the user;

See Section 1(c) above.

In addition to the methods of information retrieval described in 1(c), members of EPIC are able to conduct investigative requests, set up alerts, and check whether there is an existing alert for a license plate of interest, on behalf of EPIC-vetted users, who must have a law enforcement nexus. LPR data from the NLPRP is sent to EPIC in xml files so that EPIC can conduct investigative requests using that data. EPIC personnel can set up alerts through DEASIL, like other authorized users of the NLPRP.

As is the case for users of the NLPRP, EPIC personnel can conduct investigative requests and set up alerts for vehicles known to be associated with criminal activity or a missing person and can conduct investigative requests during a traffic stop when that investigative request is done in furtherance of the traffic stop mission. In addition, EPIC personnel can conduct investigative requests on behalf of DEA users who are investigating the travel history of a person working as a confidential informant. When EPIC personnel conduct an investigative request using the xml data, they receive the following information regarding the license plate of interest: date(s)/time(s) of license plate sightings in the last 90 days, locations of those sightings, pictures of those sightings (if available), whether there is an existing alert for the license plate, and, if there is, the point of contact relating to that alert. The results

contain a confidence percentage for the match between the license plate of interest and the license plate number recognized by the LPR.

(f) how information is transmitted to and from the system;

Information is transmitted to the NLPRP from DEA-owned LPRs and LPRs owned by state or local law enforcement entities. DEA-owned LPRs are directly linked to the NLPRP. LPRs owned by law enforcement entities other than DEA may be connected to the NLPRP by direct link, by using a virtual private network, or by using a server to which both DEA and the other law enforcement agency have access. As noted above in Section 1(e), LPR data from the NLPRP is sent to EPIC in xml files so that EPIC can conduct investigative requests using that data.

The types of information entered by a user to conduct an investigative request or create an alert are described in Section 1(c) above. The types of information received in response to an investigative request, alert, or deconfliction request is also described in Section 1(c). Information responsive to investigative requests and alerts is transmitted to DEA users through DEASIL and to non-DEA users through DICE or DEASIL.

(g) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects);

DEASIL is a web gateway portal to the NLPRP. DEASIL consolidates and streamlines customers' access into these web-based applications providing a secure, direct, remote, internal/external connectivity. DEASIL is accessible from DEA's Firebird internal network and from the external Internet via a web browser. The DEASIL application is a Sensitive But Unclassified (SBU) system that is hosted on the Speedway/U infrastructure managed by DEA.

DEASIL has an interconnection with DEA's DICE deconfliction legacy system to provide limited historical and deconfliction notification functions through DICE, but DICE improvements are underway, which will eliminate the interconnection from DEASIL to DICE. Once complete, the legacy DICE system will no longer maintain an interconnection with DEASIL.

(h) Whether it is a general support system, major application, or other type of system.

NLPRP is classified as a minor application under Speedway/U General Support System. Direct access for role-based users to the NLPRP is achieved through the DEASIL application.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security		Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID	x	Credit card			
Other identifying numbers (specify): License plate numbers					

General personal data					
Name	*, ***x	Date of birth	*x	Religion	
Maiden name	*x	Place of birth	*x	Financial info	
Alias	*x	Home address	*x	Medical information	*x
Gender	**x	Telephone number	*x	Military service	
Age	**x	Email address	*x	Physical characteristics	**x
Race/ethnicity	**x	Education	*x	Mother's maiden name	*x

Other general personal data (specify):

∗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. These photographs are not passed through any type of facial recognition system.

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

Work-related data					
Occupation	*x	Telephone number	*, **x	Salary	
Job title	*x	Email address	*, **x	Work history	
Work address	*x	Business associates	*x		

Work-related data
Other work-related data (specify): *The LPR cameras do not collect this information. Rather, an NLPRP user may 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. ** The LPR cameras do not collect this information. Rather, an NLPRP user will enter this information for himself or herself, a secondary agent, and/or a supervisor when using the NLPRP.

Distinguishing features/Biometrics					
Fingerprints		Photos	x	DNA profiles	
Palm prints		Scars, marks, tattoos	*x	Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify): *This information may be included in the remarks field of 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, 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. These photographs are not passed through any type of facial recognition system.					

System admin/audit data					
User ID	X	Date/time of access	x	ID files accessed	x
IP address	X	Queries run	x	Contents of files	x
Other system/audit data (specify):					

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax		Online	x
Telephone	x	Email			
Other (specify):					

Government sources					
Within the Component	x	Other DOJ components	x	Other federal entities	x

Government sources					
State, local, tribal	x	Foreign	x		
Other (specify):					

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

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.

The NLPRP is carefully implemented and managed to minimize the impact on personal privacy, and to ensure compliance with the Constitution and applicable laws. There is always some potential risk to privacy when the government collects information about an individual. The risk is heightened if the government keeps that information indefinitely or uses or shares it for reasons incompatible with the purposes for which the information was appropriately collected. Such risks are mitigated by the NLPRP. The information collected by the NLPRP is limited in scope, retained for a limited duration, and used and shared in a manner consistent with this privacy impact assessment and, when applicable, the Privacy Act and the routine uses in the SORN, Investigative Reporting and Filing System, 77 Fed. Reg. 21,808 (April 11, 2012). NLPRP information is accessed only by authorized users who obtain from the system information about license plates associated with suspected criminal activity or missing persons or that is relevant to the mission of a traffic stop. The vast majority of NLPRP information is never accessed. All images and data in the NLPRP system become inaccessible to users within 90 days from the date of their collection. Images and data in the NLPRP system that are determined to be relevant to an investigation are moved into and stored in an investigative case file.

Generally, the nature and quality of information can present additional risks to privacy, particularly when the individual is not the source of the information obtained about him/her. However, 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, and in some instances license plate state information, based on photographs of license

plates. The photographs themselves are available for human review. 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.

The risk of unauthorized or unnecessary access to information not pertinent to an active case or investigation is minimized because DEA has implemented numerous security controls and audit capabilities. Only authorized individuals are granted access to the NLPRP. Passwords, password protection identification features, and other system protection methods restrict access to information. Activity-based access is granted only at the level required by the individual's position. For example, a user may be given access to the system to set up an alert, but could have his or her ability to conduct investigative requests revoked if necessary.

In addition, 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. Only users who have an investigative need and a reasonable articulable suspicion that a particular license plate is involved in criminal activity or a missing person situation may or set up an alert for that license plate.

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 DICE rules of behavior. Users who violate the security procedures may be denied access to the NLPRP, DICE, or other DEA information technology systems, or face more severe civil/criminal penalties, if applicable. The NLPRP has Security Administrators who are responsible for viewing, monitoring, and archiving security logs and audit trails. Users determined to have performed unauthorized searches will have their access revoked.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
x	For criminal law enforcement activities	x	For civil enforcement activities
	For intelligence activities		For administrative matters
x	To conduct analysis concerning subjects of investigative or other interest	x	To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
[x]	For litigation		
	Other (specify):		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

The NLPRP is an investigative tool that provides law enforcement the ability to more effectively investigate and prosecute narcotics trafficking, other criminal activity, and missing person situations and to further the traffic stop mission of ensuring officer safety and investigating reasonable suspicion that arises during a traffic stop that is unrelated to the reason for the traffic stop. The NLPRP information provides law enforcement with vital investigative information regarding the locations of target vehicles. The photographic images and data collected by the NLPRP enables LEOs to confirm or discount information already gathered from sources, to locate vehicles, and to gather additional investigative information. The deconfliction functionality aids law enforcement in coordinating overlapping investigations.

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, LEOs who are mobilized for a tactical law enforcement response may receive notification that the subject vehicle is approaching their location. Alternatively, if LEOs learn the location of the subject vehicle, but are not themselves in that area, the LEOs may request a law enforcement response from LEOs in the immediate geographic area of the subject vehicle.

The information received in response to an investigative request can confirm or discount information already obtained in the investigation, provide important evidence, or create new leads. 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 up to 30 minutes before and 30 minutes after the 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. All of the above capabilities are important to DEA's mission of combatting narcotics trafficking and related offenses.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

	Authority	Citation/Reference
X	Statute	21 U.S.C. § 801 *et seq.*
	Executive Order	
x	Federal Regulation	28 C.F.R. §§ 0.100 and 0.101

x	Memorandum of Understanding/agreement	Federal, state, local, and tribal information-sharing MOUs and regional hub MOUs
	Other (summarize and provide copy of relevant portion)	

3.4 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.)

DEA users are only to retain information from the NLPRP that they determine has relevance to investigative or enforcement activities and that they place 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 DEA-008, which is published in the Federal Register, 77 FR 21808 (April 11, 2012), *available at* justice.gov/opcl/doj-systems-records. Information that is not accessed or viewed or that has been viewed and been deemed not relevant will become inaccessible within 90 days and will be purged from the system.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

The NLPRP is safeguarded in accordance with applicable laws, rules, and policies, such as DEA's automated systems security, access, and anti-virus policies. NLPRP information is maintained in buildings with restricted access. Passwords, password protection identification features, and other system protection methods also restrict access to the information. Only personnel who maintain the NLPRP and authorized users are permitted access to NLPRP information.

Several administrative and technological controls secure NLPRP information and support continuous oversight. Security Administrators are responsible for viewing, monitoring, and archiving system security logs and audit trails. User Access Managers are responsible for adding, changing, or deleting users and their access privileges.

All DEA personnel with access to DEA's information technology are required to agree to information technology rules of behavior and to complete annual security awareness training, which includes training on privacy awareness, privacy protections, and the Privacy Act. Prior to being given access to the NLPRP through DICE or DEASIL applications, state, local, and tribal users must be successfully

vetted by EPIC. Those users are recertified periodically for continued access. All non-DEA users agree to abide by the DEASIL rules of behavior. Users who violate the security procedures may have their access to the NLPRP revoked.

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.

Please see Subsection 2.3 for additional analysis concerning potential threats and mitigation strategies.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	X		X	
DOJ components	X		X	
Federal entities	X		X	
State, local, tribal gov't entities	X		X	
Public				
Private sector				
Foreign governments	X			
Foreign entities				
Other (specify):				

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

Measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient include 1) limiting access to authorized users, 2) input required by users to obtain any of the data, 3) MOUs that identify the requirements for participation in the program, including safeguards to be implemented by the recipient to ensure appropriate use of the program, 4) contracts with those responsible for protecting and maintaining the security and functionality of the program, and 5) the above-described training.

In order to guard against unauthorized disclosure, the NLPRP is safeguarded in accordance with applicable laws, rules, and policies, including DEA's automated systems security, access, and anti-virus policies. The information in the NLPRP is retained in a closed network and is accessed via permissions given to authorized users. See Sections 1(d) and 1(g) for further information about access to the system and the set-up of the system.

All investigative requests and alerts must contain identifying information for the authorized user inputting the investigative request or alert and identifying information for the person on whose behalf the request or alert is entered if that person is someone other than the authorized user inputting the request or alert. Thus, all requests and alerts can be associated with the original requestor.

See Sections 2.3 for additional analysis regarding potential threats to privacy, 3.5 for additional information regarding the use, handling, retaining, and disposal of information, and 6 for additional information regarding information security.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

	Yes, notice is provided by other means.	Specify how:
X	No, notice is not provided.	Specify why not: see explanation contained in 5.4.

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

	Yes, individuals have the opportunity to decline to provide information.	Specify how:
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: see explanation contained in 5.4.

5.3 Indicate whether and how individuals have the opportunity to consent to

particular uses of the information.

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: see explanation contained in 5.4.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

System of Records Notice DEA-008 provides general public notice of the investigative information that DEA collects in connection with mission-related activities. Additionally, signs are posted at ports of entry to notify individuals of monitoring and information collection.

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. Similarly, obtaining consent would be impractical and thwart law enforcement investigations. Information is only collected in locations where equipment has been installed with the permission of a property owner and on public roadways, where individuals generally lack a reasonable expectation of privacy.

Section 6: Information Security

6.1 Indicate all that apply.

X	**The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation**: November 17, 2017 **If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:**
X	**A security risk assessment has been conducted.**

X	**Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify:** The information is secured in accordance with FISMA requirements and resides in a closed SBU WAN General Support System. Computing equipment of the NLPRP is housed in federal facilities with limited and controlled access certified to the level of an Open Storage Area. The information itself is retained in a closed network accessible only to authorized users. Roles are assigned to determine the class of information in NLPRP to which individuals are allowed access. Access to the NLPRP is controlled using role-assigned privileges. Role-based access is determined by investigative need and granted by the system administrator after an official request is validated through the requesting agency or the individual's chain of command. Access is controlled by multiple-layer login assignment of user IDs, and assistance in resetting user-generated passwords. Access and entry logs are maintained within the NLPRP. It is required that any agency or individual requesting a change in roles or permissions present that request in written format to the system administrator. All images and data in the NLPRP become inaccessible to users 90 days after their collection and are purged from the system. All user roles are strictly read-only with no means to modify LPR-collected information. Information is protected by a one-way data diode that prevents external access to it (i.e., Non-DEA personnel). All Microsoft recommended security patches are applied during a weekly maintenance cycle. Databases that are accessible via this portal are encrypted to protect data at rest and follow industry best practices to secure the transmission of data. Non-DEA users access the NLPRP via DICE, which is accessed using a web portal that leverages an edge computing platform that provides Web Application Firewalls to protect against any malicious attacks from the perimeter. The portal leverages industry best practices of adopting DNSSEC and HTTP Strict Transport Security that supplements the existing secure transport layer. The infrastructure layout includes multiple firewalls, which separate the tiered VLAN architecture, thereby protecting the backend systems. The communication between infrastructure components is established over Transport Layer Security and hosted over a PKI-enabled infrastructure.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** See discussion of auditing procedures below. In addition, quarterly security scans are performed and all detected vulnerabilities are resolved.

X		**Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information:** DEA has procedures that allow for the auditing of the creation and modification 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 Certification and Authorization processes.
X		**Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.**
X		**Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.**
X		**The following training is required for authorized users to access or receive information in the system:**
		General information security training
		Training specific to the system for authorized users within the Department.
		Training specific to the system for authorized users outside of the component.
	X	**Other (specify):** DEA employees 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 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

See Sections 1(d), 1(g), 2.3, 3.5, 4.2, and 6.1, above.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

x	Yes, and this system is covered by an existing system of records notice. SORN for DEA's Investigative Reporting and Filing System, DEA-008, most recently published in full on April 11, 2012, at 71 FR 21,808. DEA is in the process of amending DEA-008 which will include updates reflecting the NLPRP.
	Yes, and a system of records notice is in development.

	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Information about United States citizens and/or lawfully admitted permanent resident aliens is retrieved as described in detail in Section 1(c).

Section 8: Civil Liberties

8.1 Indicate whether the system is consistent with civil liberties principles.

The NLPRP is consistent with civil liberties protections under the First and Fourth Amendments. For example, information is collected for authorized law enforcement purposes and is not collected on the basis of race, gender, national origin, sexual orientation, or gender identity. The NLPRP is consistent with the Department's 2014 Use of Race Policy ("Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity"), which defines the limited circumstances in which race, ethnicity, gender, and other characteristics may be taken into account by federal law enforcement officers. The NLPRP may not be used for monitoring members of the public regarding the exercise of their First Amendment rights.

NLPRP use is only permitted in conjunction with a criminal investigation, missing person situation, or traffic stop. Information in the system becomes inaccessible 90 days after its collection and is purged from the system. Only information relevant to a DEA investigation is to be transferred to the DEA case file for retention in that case file.

Moreover, the collection of data in the NLPRP does not constitute a Fourth Amendment search or seizure. The information contained in the NLPRP is publicly viewable information in which individuals lack a reasonable expectation of privacy. The information is publicly accessible, and no trespasses occur to obtain the information.