License Plate Reader

Policy Development Template

For Use in **Intelligence and Investigative Activities**

February 2017

Where to Locate This Resource

This resource is available online at www.it.ojp.gov/privacy and at www.ncirc.gov. To request printed copies, send requests to information@ncirc.gov.

To Request a Word Version of the Template

To request a Word version, send requests to information@ncirc.gov.

This project was supported by Grant Number 2013-D6-BX-K001, awarded by the Bureau of Justice Assistance, in collaboration with the U.S. Department of Homeland Security. The Bureau of Justice Assistance is a component of the Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice or the U.S. Department of Homeland Security.

License Plate Reader Policy Development Template for Use in Intelligence and Investigative Activities

February 2017

Table of Contents

Introduction

Automatic license plate readers (ALPRs)—also known as license plate readers (LPRs)—use image-processing technology to identify vehicles by their license plates. LPRs automate a process that, in the past, was conducted manually by officers, license plate by license plate, with much officer discretion. Using a special form of optical character recognition (OCR), the LPR's algorithms transform pixels of a digital image into the text of a license plate. Since entering the market, LPRs have been employed in many applications, but one of the fastest-growing uses is by justice entities who use LPR technology as an investigative tool to aid them in recovering stolen vehicles, locating possible criminals, assisting in the security of large public venues, and conducting other intelligence and investigative activities. Images are captured by LPRs and translated into letters and numbers and compared to law enforcement databases of registered vehicles, including those known to be or suspected of being involved with crimes or infractions. If a match to possible criminal activity is found, the LPR system provides an alert to the officer that a suspected vehicle is in the immediate area of an LPR.

Through this growing adoption of LPRs, justice entities are reporting increased successes in locating stolen vehicles and identifying suspects. Dale Stockton, Program Manager, Road Runner, Automated Regional Justice Information System, San Diego, shared the following with attendees at a National Institute of Justice conference:

> This is the best tool we've had come along in a very long time. It can really impact crime. It can really impact public safety. . . . And, although it's often used for locating stolen cars, the reality is . . . the value goes far beyond stolen cars, particularly in the area of investigative support. . . . The biggest reason that we want to use LPR in the field, though, is that it truly is a force multiplier. Officers can do their normal job on patrol and the license plate reader functions in the background while the officer pays attention to what's going on around them. . . . One of the more recently realized applications is in support of homeland security because, around this country, we have identified infrastructure that we know is at risk . . . so if we start looking at vehicles frequenting that infrastructure, that can give us greater insight as to where potential risks are.[1]

News stories, like the ones listed below, are increasing, demonstrating the kinds of success justice entities have had in using LPRs:

- "A Look at Plate Readers That Helped Officer Catch Murder Suspect in West Carthage," WWNYTV 7, July 3, 2016.
- "Suspect in a Hit-and-Run Death of 9-Year-Old Girl Located Using Historical and Commercial License Plate Reader Data," PR Newswire, Livermore, California, March 31, 2016.
- "License Plate Readers Used to Find Journalist Killer Also Used in WNY," WIVB News Channel 4, Buffalo, New York, August 27, 2015.
- "Queens Man Pleads Guilty to Manslaughter in Death of Roommate's Friend," Office of Richard A. Brown, District Attorney, Queens County, New York, November 4, 2011.

"This is a great tool for us," said a New York State Trooper in an interview on license plate readers used to locate a suspect in shooting deaths of two journalists. "If it was a suspended plate, an alarm would go off on here saying registration suspected or revoked, and at that point in time I would have to make sure the plate that was read is the correct plate . . . . It is a great tool for law enforcement; it's a great tool for the community."[2]

[1] National Institute of Justice (NIJ) Audio Transcript: Using License Plate Readers to Fight Crime, www.nij.gov.
[2] "License Plate Readers Used to Find Journalist Killer Also Used in WNY," George Richert, News 4 Reporter, WIVB News Channel 4, Buffalo, New York, August 27, 2015, http://wivb.com/2015/08/27/license-plate-readers-found-virginia-suspect/.

Even with the proven efficacy of this technology, justice entities should be alert to risk of erroneous or deficient LPR data:

- "Driver Finds Himself Surrounded by Cops With Guns Out After Automatic License Plate Reader Misreads His Plate," TechDirt, April 28, 2014.
- "License Plate Reader Error Leads to Traffic Stop at Gun Point, Court Case," Ars Technica, May 12, 2014.

Justice entities should therefore put in place appropriate policies and procedures to guard against possible errors and other potential problems. Strong control and oversight are critical considerations in policy development, especially as the civil liberties implications of possible unforeseen derivative uses may be significant. Such efforts will not only enhance mission effectiveness but also safeguard privacy, civil rights, and civil liberties of individuals.

A. License Plate Reader (LPR) Policies

As illustrated by the successes described earlier, justice entities (such as law enforcement or homeland security agencies, fusion centers, and intelligence units) are turning to LPR technology more and more. However, when considering or implementing an LPR program, individual privacy, civil rights, and civil liberties must also be vigorously protected. Establishing and implementing such protections in an entity's LPR policy will help guide the justice entity's LPR information collection, receipt, access, use, dissemination, retention, and purging efforts. Such proactive work supports and enhances the justice entity's ability to both fulfill its mission while also protecting the privacy, civil rights, and civil liberties of community members—strengthening trust and public confidence through effective and responsible use of LPR technology.

When an entity determines to develop and implement an LPR policy, it is important to note that such a policy is not a one-time project; it is one component of an ongoing LPR program that works to protect privacy, civil rights, and civil liberties. As agencies consider establishing and implementing a policy for LPR information, they are encouraged to consider the LPR policy as one in a series of the following steps:

1. Educate and raise awareness on the importance of having privacy, civil rights, and civil liberties protections.
2. Assess agency privacy, civil rights, and civil liberties risks by evaluating the process through which the agency collects, receives, accesses, uses, disseminates, retains, and purges LPR information.
3. **Develop an LPR policy** to articulate the legal framework and policy position on how the agency handles LPR information.
4. Perform a policy evaluation, prior to publishing, to determine whether the policy adequately addresses current standards, privacy protection recommendations, and the law.
5. Implement and train personnel and authorized users on the established rules and procedures.
6. Perform an annual policy review and make appropriate changes in response to implementation experience, guidance from oversight or advisory bodies, applicable law, technology, and public expectations.
7. Audit the processes described in the LPR policy.

A comprehensive LPR policy that is developed in a transparent manner and properly enforced fosters trust—not only within and between justice partners but also by the public, whose LPR information may be collected and utilized. This process thus ensures that justice entities are serving as responsible stewards of LPR information and operating with respect for individual privacy and the law. Without this trust, LPR program initiatives may give rise to additional public scrutiny and civil liability.

To support justice entities in their efforts to implement LPR policies and procedures, the following policy development template was developed by state, local, and federal law enforcement and criminal justice partners and is designed to assist justice entity personnel—whether in a law enforcement or homeland security agency, a fusion center, or an intelligence unit—in developing a comprehensive LPR policy.

Justice entities (law enforcement and homeland security agencies, fusion centers, intelligence units, etc.) utilize different types of information (e.g., criminal history, suspicious activity reports [SARs]) and intelligence (e.g., criminal intelligence information) as part of their intelligence or investigative activities. Each type of information and intelligence is governed by laws, regulations, and policies. LPR information, as collected and maintained in an LPR database, is not considered intelligence, criminal history, or SAR information. As such, the laws, regulations, and policies that apply to those types of information and intelligence may not apply to LPR information until such time as it is downloaded and incorporated into an intelligence or investigative case file. The digital image of license plates is maintained in a separate database from all other types of information and does not include additional information that identifies a particular individual. License plate numbers and date/time location collected through an LPR are not, when taken alone, sufficient to identify the individual associated with the vehicle. Even though the LPR information accessed by the justice entity results from an LPR system's automated collection of license plate numbers, it is the investigative and/or analytic process that associates the stored digital license plate image with an identifiable individual.

For these reasons, this policy template was developed to address the collection, receipt, access, use, dissemination, retention, and purging of LPR information that is not yet part of an intelligence or investigative file. Once LPR information is downloaded by entity personnel and incorporated into an intelligence or investigative file, the LPR information is then considered intelligence or investigative information and the laws, regulations, and policies applicable to that type of information or intelligence govern its use.

The provisions suggested in this template are intended to be incorporated into the entity's general operational policies and day-to-day operations and to provide explicit and detailed privacy, civil rights, and civil liberties protection guidance to entity personnel and other authorized source and participating agencies. This policy template was developed based on the core principles articulated in the Fair Information Practice Principles (refer to Appendix B). Each section is a fundamental component of an overall comprehensive LPR policy that includes vital baseline provisions on legal compliance, governance and oversight, acquiring and receiving, use, sharing and dissemination, information quality, redress, security and maintenance, retention and purging, accountability and enforcement, and training concepts.

B. How to Use This Template

This template is designed with policy concepts grouped into related sections. Each section contains pertinent policy provision questions shown in **bold** type. Sample policy language is shown under each question in regular type.

1. Different Entity LPR Roles

There are generally two different ways (or roles) entities come into contact with LPR information:

- Entities that do not collect LPR information but have access to and query an LPR database.
- Entities that actively collect, receive, access (query), disseminate, retain, and purge LPR information.

The policy provisions contained in this template were designed to be customized for either role. Entities that do not collect, receive, and retain LPR information but only access and query an LPR system will find that some provisions may not apply. However, all of the provisions will most likely apply, in some form, to entities that do collect, receive, and retain LPR information. Notations are provided within each applicable provision to allow for customization according to these entity roles.

2. Referencing Other Policies

Frequently, agencies already have established privacy-related policies and practices contained in broader policy documents (e.g., concept of operations, standard operating procedures, user agreements, and employee handbooks). In accordance with template Sections L, Accountability and Enforcement, and L.1, Transparency, agencies are strongly encouraged to make their LPR policies available to the public, even if the other existing policies are not made available publicly. As such, consolidating various existing LPR policy provisions contained in other documents into one LPR policy is highly recommended. Agencies are cautioned, however, against simply providing a cross-reference to other policies in effect. Cross-referencing, without including the applicable policy language, should be done only if those policies are also available to the public; otherwise, agencies should restate (or excerpt) the applicable language within their LPR policy.

3. Template Modifications—Customizing Your Policy

It is important to note that this policy development template is not intended to be used as is, without modification. Each section represents the foundational components of an effective LPR policy but does not cover all concepts that may be particular to your entity, its unique processes and procedures, or the applicable constitutional provisions, laws, ordinances, or regulations within your state. Further, certain concepts or questions may not be applicable. The template represents a starting point for your entity to establish minimum baseline LPR policy protections. Law enforcement entities are encouraged to complete as many of the template questions as are applicable and to enhance sections to include items such as references to applicable statutes, rules, standards, or policies and to provide additional sections for provisions that are not addressed.

While it is important for entities to review each question and associated guidance contained in the policy template section of this document, a sample LPR policy that incorporates all of the sample policy language contained in the template section is provided in Appendix E for ease of customization.

C. Resource List

Resources that may be of interest include:

- *Acceptable Use Policy for the Regional License Plate Reader System*, Automated Regional Justice Information System (ARJIS), www.arjis.org/RegionalPolicies/ARJIS%20LPR%20AUP%20-%20Approved%20-%20Rev150213.pdf.
- Automated License Plate Reader Frequently Asked Questions, International Association of Chiefs of Police (IACP), www.iacp.org/ALPR-FAQs.
- *Automated License Plate Readers: A Primer*, Violence Reduction Network, www.vrnetwork.org/Documents/License%20Plate%20Readers%20primer.pdf.
- *Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement*, IACP, www.ncjrs.gov/pdffiles1/nij/grants/239604.pdf.
- *Best Practices Guide for Improving Automated License Plate Reader Effectiveness Through Uniform License Plate Design and Manufacture*, American Association of Motor Vehicle Administrators (AAMVA), www.aamva.org/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=2911&libID=2897.
- Fair Information Practice Principles, refer to Appendix B.
- *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template*, U.S. Department of Homeland Security (DHS) and the U.S. Department of Justice (DOJ), April 2010, https://it.ojp.gov/documents/d/Fusion_Center_Privacy_Policy_Development_508compliant.pdf.
- *Guidelines to Ensure That the Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment* (ISE Privacy Guidelines), Office of the Program Manager, Information Sharing Environment (ISE), www.ise.gov/sites/default/files/PrivacyGuidelines20061204.pdf.
- *Initial Privacy Impact Assessment for Automated License Plate Reader Technology*, Northern California Regional Intelligence Center (NCRIC), https://northerncaliforniamostwanted.org/html/NCRIC%20ALPR%20PIA.PDF.
- *IACP Technology Policy Framework,* IACP, January 2014, www.theiacp.org/Portals/0/documents/pdfs/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf.
- *License Plate Readers for Law Enforcement: Opportunities and Obstacles*, RAND Corporation, www.rand.org/pubs/research_reports/RR467.html.
- *License Plate Recognition Technology (LPR) Impact Evaluation and Community Assessment*, George Mason University, http://cebcp.org/wp-content/evidence-based-policing/LPR_FINAL.pdf.
- *License Plate Standard,* American Association of Motor Vehicle Administrators, 2016, www.aamva.org/licenseplatestandard_2016/.
- *Mobile License Plate Reader System Standard for Law Enforcement Working Draft,* NIJ Standard-100x.00, National Institute of Justice, Office of Justice Programs (OJP), DOJ, August 21, 2014, www.justnet.org/pdf/Draft_Mobile_License_Plate_Reader_System_Standard_for_Law_Enforcement.pdf.
- *Privacy, Civil Rights, and Civil Liberties Audit Guidance for the State, Local, Tribal, and Territorial Intelligence Component*, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/181/Privacy--Civil-Rights--and-Civil-Liberties-Audit-Guidance-for-the-State--Local--Tribal--and-Territorial-Intelligence-Component.
- *Privacy Impact Assessment for the Acquisition and Use of License Plate Reader Data From a Commercial Service*, U.S. Department of Homeland Security, www.dhs.gov/publication/dhs-ice-pia-039-acquisition-and-use-license-plate-reader-data-commercial-service.
- *Privacy Impact Assessment Report for the Utilization of License Plate Readers*, IACP, www.theiacp.org/Portals/0/pdfs/LPR_Privacy_Impact_Assessment.pdf.
- *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies*, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/35/Recommendations-for-First-Amendment-Protected-Events-for-State-and-Local-Law-Enforcement-Agencies.

License Plate Reader (LPR) Policy Development Template for Use in Intelligence and Investigative Activities

A. Purpose Statement

1. What is the purpose of establishing a license plate reader (LPR) policy (i.e., what does the entity hope to accomplish in adopting this policy)? Provide a succinct, comprehensive statement of purpose.

It is the purpose of this policy to provide **[name of entity]** personnel with guidelines and principles for the collection, access, use, dissemination, retention, and purging of LPR information to ensure that the information is used for legitimate law enforcement purposes only and the privacy, civil rights, and civil liberties of individuals are not violated. The Fair Information Practice Principles (FIPPs) form the core of the privacy protection framework for this policy.

This policy assists **[name of entity]** and its personnel in:

- Increasing public safety and improving state, local, tribal, territorial, and national security.
- Minimizing the threat and risk of injury to specific individuals.
- Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.
- Promoting governmental legitimacy and accountability.
- Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
- Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information.
- Minimizing the threat and risk of damage to real or personal property.
- Increasing trust by maximizing transparency.
- Making the most effective use of public resources allocated to public safety entities.

2. What are the entity's authorized uses for LPR information?

The provisions of this policy are provided to support authorized uses of LPR information. Authorized uses may include the following **[include any of the following purposes or others that apply to the entity]**:

- Enhance **[insert state]**'s AMBER/SILVER or other law enforcement alerts and real-time response capability by deploying and networking LPRs across the state to more rapidly identify and locate vehicles related to potential child-abduction or other serious crimes.
- Alert law enforcement that a particular license plate on a "hot list" (e.g., a stolen vehicle or a vehicle associated with a wanted individual) is in close proximity to an LPR to dramatically reduce the recovery time of stolen vehicles and assist in locating dangerous and wanted individuals.
- Identify plates associated with potential witnesses and/or victims of violent crime.

- Support **[name of entity]**'s homeland security mission by protecting critical infrastructure from individuals who intend to damage or disrupt the systems and locations that allow for travel and the free flow of commerce.
- Identify vehicles linked to stolen license plates or other motor vehicle traffic violations.
- Provide situational awareness for law enforcement related to public safety or otherwise relevant to their authorized duties.
- Support local, state, federal, and tribal public safety departments in the identification of subjects associated with/as targets of criminal investigations.
- Support law enforcement response to critical incident responses and special events.
- Support special operations, such as high-crime-area patrols, gang investigation/suppression, driving under the influence initiatives, enforcement details, directed criminal investigations, and other investigations.

B. Policy Applicability and Legal Compliance

1. What information is subject to the LPR policy?

This policy applies to LPR information collected or received, accessed, used, disseminated, retained, and purged by the **[name of entity]**. It is not intended to apply and does not apply to any other types of information accessed, retained, or used by the **[name of entity]**.

2. Who is subject to the LPR policy? Identify who must comply with the LPR policy; for example, entity personnel, participating agencies, and private contractors.

All **[name of entity]** personnel, participating agency personnel and authorized individuals working in direct support of **[name of entity]** personnel (such as interns), personnel providing information technology services to the **[name of entity]**, private contractors, and other authorized users will comply with the **[name of entity]**'s LPR policy. This policy applies to information the **[name of entity]** collects or receives, accesses, uses, disseminates, retains, and purges.

3. How is the entity's LPR policy made available to personnel, participating entities, and individual users (in print, online, etc.), and are acknowledgment of receipt and agreement to comply with this policy required in writing?

The **[name of entity]** will provide a printed or electronic copy of this LPR policy to all:

- **[name of entity]** and non-**[name of entity]** personnel who provide services.
- Participating agencies.
- Individual authorized users.

The **[name of entity]** will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the applicable provisions it contains.

4. This entity requires *personnel and participating information-originating and user agencies* to be in compliance with all applicable constitutional and statutory laws. What are the primary laws with which personnel and participating agencies must comply?

Cite the primary laws with which personnel and participating users must comply that protect privacy, civil rights, and civil liberties in the collection, receipt, access, use, dissemination, retention, and purging of LPR information.

This should include any state statute regarding deployed LPR systems by state or local government. It might also include the U.S. Constitution and state constitutions; open records or sunshine laws; information breach notification laws; other laws, regulations, orders, opinions, or policies impacting or protecting privacy, civil rights, or civil liberties; local ordinances; and relevant federal laws, such as the Driver's Privacy Protection Act and regulations. (For synopses of primary federal laws an entity should consider referencing in the LPR policy, refer to Appendix C, Listing of Federal Laws.)

All **[name of entity]** personnel, participating agency personnel and authorized individuals working in direct support of **[name of entity]** personnel (such as interns), personnel providing information technology services to the **[name of entity]**, private contractors, agencies from which **[name of entity]** information originates, and other authorized users will comply with applicable laws and policies concerning privacy, civil rights, and civil liberties, including, but not limited to **[include a specific reference to any relevant state statutes or other binding state or local policy specific to LPR systems, then provide a list of other applicable state and federal privacy, civil rights, and**

civil liberties laws or include a reference to the section or appendix containing a list of applicable laws]. As part of this process, all individuals working with LPR information will complete the applicable training as directed by **[name of entity]**.

C. Governance and Oversight

1. **Who has primary responsibility for the entity's overall operation, including the entity's justice information systems, information collection and retention procedures, coordination of personnel, and enforcement of this policy? Which individual will ultimately be held accountable for any problems or errors?**

   Primary responsibility for the operation of the **[name of entity]**; its justice information systems, operations, and the coordination of personnel; the receiving, seeking, retention, evaluation, information quality, use, purging, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the **[position/title]** of the **[name of entity]**.

2. **Who is assigned primary responsibility for overseeing and administering the entity's LPR program?**

   The **[name of entity]**'s **[insert title]** will designate an LPR Administrator who will be responsible for the following **[include any of the following responsibilities that apply to the LPR Administrator or other responsibilities]**:

   - Overseeing and administering the LPR program.
   - Ensuring that stored LPR information is automatically purged from the LPR database, unless determined to be of evidentiary value (refer to Section K.1, Information Retention and Purging).
   - Confirming, through random audits, that LPR information is purged in accordance with this policy.
   - Acting as the authorizing official for individual access to LPR information.
   - Ensuring and documenting that all personnel with authorized access to LPR information are trained prior to using the system.
   - Conducting audits to ensure compliance with applicable laws, regulations, standards, and policy.

3. **What is the process for developing, reviewing, and updating the LPR policy?**

   The **[name of entity]** is guided by a **[insert guiding authority, for example, a "designated LPR oversight committee"]** that liaises with the community to ensure that privacy, civil rights, and civil liberties are appropriately protected by this LPR policy and by the **[name of entity]**'s LPR information collection, receipt, access, use, dissemination, retention, and purging processes and procedures.

   Approach 1: The committee will annually review and update the LPR policy in response to changes in law and implementation experience, including the results of audits and inspections, and will solicit input from stakeholders on the development or proposed updates to the LPR policy.

   Approach 2: The committee will annually review and update the LPR policy in response to changes in law and implementation experience, including the results of audits and inspections, and will provide notice to and solicit comment from the public on the development or proposed updates to the LPR policy.

4. **Who is the designated and trained privacy, civil rights, and civil liberties individual or entity who will handle reported errors and violations and oversee the implementation of LPR privacy, civil rights, and civil liberties protections?**

   [Provide the title of the individual or name of the entity. This may be the privacy, civil rights, and civil liberties officer; legal counsel; internal affairs; external entities such as the U.S. Attorney or the Office of Inspector General; or other.]

   The **[insert title of individual or name of entity]** will receive reports regarding alleged errors and violations of the provisions of this LPR policy, will receive and coordinate complaint resolution under the **[name of entity]**'s LPR redress policy, and will ensure that privacy, civil rights, and civil liberties protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The **[insert title of individual but not the name or name of entity]** may be contacted at the following address: **[insert mailing address or e-mail address]**.

5. **Who is responsible for ensuring that enforcement procedures and sanctions for noncompliance with the LPR policy are adequate and enforced?**

   The **[name of entity]**'s **[insert title]** will ensure that enforcement procedures and sanctions outlined in **[insert section number of policy (see Section L.3, Enforcement)]** are adequate and enforced.

D. Definitions

1. **What key words or phrases are regularly used in the LPR policy for which the entity wants to specify particular meanings?**

   This may include terms that are not commonly known or have multiple meanings that may need to be clarified to indicate which one applies to the LPR policy. There may be legal definitions for terms in the statutes governing the operation of justice information or LPR systems. For examples of definitions of key terms commonly used throughout this template, refer to Appendix A, Glossary of Terms and Definitions.

   For examples of primary terms and definitions used in this LPR policy, refer to **[insert section or appendix citation]**.

E. Acquiring and Receiving LPR Information

1. **Describe how the entity acquires LPR information. Use the following provisions that apply to the entity. If neither a. nor b. applies because the entity does not directly collect or indirectly acquire LPR information, skip question 1 and move to question 2. For entities that do directly collect and/or indirectly acquire LPR information, answer the applicable question but also answer question 2, since it is understood that the entity would also query such information.**

   a. **If the entity directly collects LPR information through LPR systems (mobile or stationary), list the authorized purpose upon which that collection is based. Note: State law may restrict collecting LPR information from commercial databases.**

      The **[name of entity]**, through its **[insert name of the entity's LPR program]**, will directly collect and retain LPR information that:

      - Is based on a potential threat to public safety or the enforcement of the criminal law, or
      - Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity, or
      - Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences, or
      - Is directly related to an investigation or mission of the law enforcement entity, and
        - The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
        - The information was collected in a fair and lawful manner (e.g., it does not infringe on the federal or state constitutional rights of any individual, group, or organization).

   b. **Does the entity indirectly acquire LPR information from other law enforcement agencies? If yes, identify the mechanism by which this occurs (e.g., memorandum of understanding [MOU], law, intergovernmental agreement [IGA]).**

      The **[name of entity]** will indirectly acquire LPR information from **[list other law enforcement agency or agencies]** in accordance with **[insert mechanisms, e.g., MOU, law, intergovernmental or interagency agreement]** established between the **[name of entity]** and the law enforcement agency(ies).

2. **For queries of LPR information, list the authorized purpose on which queries are based. Indicate whether the entity queries a law enforcement or commercial database or both. Note: State law may restrict queries to commercial databases.**

   The **[name of entity]** will query **[insert name of law enforcement or commercial database]** LPR information that:

- Is based on a possible threat to public safety or the enforcement of the criminal law, or
- Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity, or
- Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime, or
- Is directly related to an investigation or mission of the law enforcement entity, and
  - The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
  - The information was collected in a fair and lawful manner (e.g., it does not infringe on the federal or state constitutional rights of any individual, group, or organization).

3. Does the entity utilize hot lists (alert lists), and if so, what is the entity's procedure?

Hot-list information is considered confidential information to the extent permitted by law and will be updated **[insert time period(s)]** each day. Officers assigned an LPR unit are responsible for ensuring they are operating with the most current hot list (at minimum) at the beginning of each shift, including information files of stolen and "of interest" vehicles containing all of the current National Crime Information Center (NCIC) information. Department members will query their LPR system to ascertain whether there is a prior read of the license plate that is the subject of the particular alert, bulletin, or alarm. Proactive manual entry of LPR hot lists in the field is permitted for:

- Dispatched reports of crimes—"Be On the Lookouts" (BOLOs) or AMBER, SILVER, or other law enforcement alerts in which a license plate number is part of the broadcast; or
- When directed or authorized for a legitimate law enforcement purpose.

4. Identify what LPR information *may not* be sought, retained, shared, or disclosed by the entity.

This may include federal or state constitutional prohibitions or prohibitions in federal, state, local, or tribal laws.

The **[name of entity]** and any information-originating entities will not seek, submit, or retain LPR information about individuals or organizations based solely on their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, gender identity, sexual orientation, or other classification protected by law.

5. Identify what information is *contained* in entity-accessed LPR information.

[Name of entity] LPR cameras may be mobile (mounted on vehicles) or stationary (i.e., mounted to a structure). A standard LPR record contains, at a minimum, an optical character recognition (OCR) interpretation of the captured image, a photo of the license plate and a contextual photo of an area surrounding the plate that could range from a few inches to a larger area around the entire vehicle, the geographic coordinates of where the image was captured, the date and time of the recording, and the specific camera/unit that captured the image.

6. Identify what information is *not contained* in entity-accessed LPR information.

[Name of entity]-accessed LPR information contains images of license plates that are available to public view (e.g., vehicles that are on a public road or street or that are on private property but whose license plates[s] are visible from a public road, street, or place to which members of the public have access, such as the parking lot of a shop or other business establishment) and that identify specific vehicles. Retained LPR information does not include specific identification of individuals. Separate video surveillance images of the same location or images from private cameras will not be associated with LPR data unless a specific image is required to investigate or document a violation in accordance with the authorized purposes described in this section.

License plate numbers and date/time location collected through an LPR may not be, when taken alone, sufficient to identify the individual associated with the vehicle. The **[name of entity]** may be able to link the LPR information to an individual through additional use and combination with other information, such as a check of vehicle registration. Thus, even though the LPR information the **[name of entity]** accesses may be the result of an LPR system's automated collection of license plate numbers, it is the investigation process that identifies individuals. Refer to Section H.2 for information on the **[name of entity]**'s LPR validation procedure or to Appendix A, Glossary of Terms and Definitions, for more information on LPR information.

Approach 1: [This approach should be used by entities that withhold LPR information from public release using the privacy exemption under the public records laws.]
The **[name of entity]** protects all LPR information as personally identifiable information (PII) because LPR information may be combined with other information to specify a unique individual (i.e., the identity of an individual could be directly or indirectly inferred by using information that is linked or linkable to that individual). The **[name of entity]** collects, receives, accesses, uses, disseminates, retains, and purges LPR information because it can be linked to an individual to further an authorized mission.

Approach 2:
In the absence of the investigation process, the license plate number and the time and location data attached to it may not identify a specific person. Thus, even though the **[name of entity]**'s LPR systems automate the collection of license plate numbers, it is the investigation process that identifies individuals. Refer to Section H.2 for information on the **[name of entity]**'s LPR validation procedure or to Appendix A, Glossary of Terms and Definitions, for more information on LPR information.

Databases of LPR information do not contain alert lists based on strictly civil matters. In addition, LPR information does not contain audio recordings.

7. **Does the LPR policy specifically require a consideration of nondiscriminatory intent in the placement of stationary cameras?**

   Per the **[name of entity]** policy of nondiscrimination noted in Section E.4, the pattern and frequency of stationary camera placement will be assessed **[note frequency]** to confirm nondiscriminatory placement.

8. **Who owns the entity's LPR hardware, software, and LPR information collected?**

   The hardware and software licenses associated with the **[name of entity]**'s LPR system are the property of **[insert name of owning agency]**, regardless of whether the system has been purchased, leased, or acquired as a service. All deployments of the LPR system are for official use only (FOUO). All information captured, stored, generated, or otherwise produced by an LPR system is the property of the **[insert name of owning agency]**, regardless of where the information is housed or stored.[3]

9. **What is the entity's policy regarding the investigative techniques the entity will follow when acquiring LPR information (for example, an intrusion-level statement)?**

   LPR information collection and investigative techniques used by the **[name of entity]** and by LPR information-originating agencies must be the least intrusive as necessary in the particular circumstances to collect LPR information the **[name of entity]** is authorized to seek or retain.

10. **If the entity contracts with commercial LPR databases, does the entity require an assurance that the commercial LPR database company is in legal compliance in its information collection, receipt, access, retention, dissemination, and purging procedures?**

    The **[name of entity]** will contract only with commercial LPR database companies that provide an assurance that their methods for collecting, receiving, accessing, disseminating, retaining, and purging LPR information comply with applicable local, state, tribal, territorial, and federal laws, statutes, regulations, and policies and that these methods are not based on misleading information collection practices.

11. **From what sources (nongovernmental, commercial, or private agencies or institutions or classes of individuals) will the entity not seek, receive, accept, or retain LPR information?**

    The **[name of entity]** will not directly or indirectly seek, receive, accept, or retain LPR information from:

    - An individual who or nongovernmental agency that may receive a fee or benefit for providing the LPR information, except as expressly authorized by law or **[name of entity]** policy, and/or
    - An individual who or information provider that is legally prohibited from obtaining or disclosing the LPR information.

[3] Refer to state law regarding ownership and compliance with open record requests regarding LPR information.

F. Use of LPR Information

1. Describe the authorized uses justifying access to or disclosure of LPR information *within the entity or in other governmental agencies*.

Access to or disclosure of LPR information will be provided only ***to individuals within the entity or in other governmental agencies*** who are authorized to have access and only for legitimate law enforcement purposes (e.g., enforcement, reactive investigations) and to IT personnel charged with the responsibility for system administration and maintenance. This means that queries and dissemination of LPR information are permitted only if:

- There is a legal basis requiring these actions, or
- There is reasonable suspicion that an individual or enterprise is involved in criminal conduct or activity, and
  - The LPR information is relevant to that suspected criminal conduct or activity and the requestor has a legitimate need to know.

Examples of legitimate law enforcement purposes to access LPR information may include:

- Enforcement
- Reactive investigations
- Supervisory or security oversight of LPR system and data use

Authorized uses are described in A.2 of this policy. However, the **[name of entity]** accords special consideration to the collection of LPR information relating to First Amendment-protected events and will articulate a legal or justified basis for such collection during the planning assessment and approval process for the particular event, before proceeding with the collection.[4]

2. Which LPR program or LPR information uses are prohibited by the entity?

The **[name of entity]** will prohibit access, use, or dissemination of LPR information for:

- Any purpose that violates the Constitution or laws of the United States, including the protections of the Fourth Amendment.
- Non-law enforcement or personal purposes.
- Discriminatory purposes.
- The purpose of prohibiting, infringing upon, or deterring activities protected by the First Amendment, such as freely practicing one's religion, freedom of speech and peaceful assembly, freedom of the press, and the right to petition the government for the redress of grievances.[5]
- The purpose of prohibiting or deterring lawful individual exercise of other rights, such as freedom of association, implied by and secured by the U.S. Constitution or any other constitutionally protected right or attribute.
- Harassing and/or intimidating any individual or group.
- Targeting of any individual or group by means of camera placement or data use in a discriminatory manner, noted in Section E.4.
- Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

3. What types of user actions and permissions are controlled by the entity's LPR access limitations?

<u>Best Practice</u>: Least privilege administration is a recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform. It is suggested that entities specify their method for identifying user actions and permissions as it relates to LPR information within their LPR policies.

In addition, the **[name of entity]** will employ credentialed, role-based access criteria, as appropriate, to control:

- The LPR information to which a particular group or class of users may have access based on the group or class.
- The assignment of roles (e.g., administrator, manager, operator, and user).

[4] For further information about these processes, see *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies* at 4, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/35/Recommendations-for-First-Amendment-Protected-Events-for-State-and-Local-Law-Enforcement-Agencies.
[5] Ibid. at 6–7 and 11–13.

- The categories of LPR information that a class of users are permitted to use in order to update a hot list, including information being utilized in specific investigations.
- Any administrative or functional access required to maintain, control, administer, audit, or otherwise manage the information or equipment.

G. Sharing and Dissemination of LPR Information

1. Under what conditions will the entity provide external law enforcement agencies with access to the entity's LPR information?

The **[name of entity]** will establish requirements for any external agency requesting access to the **[name of entity]**'s LPR information. These requirements will be documented in an interagency agreement/memorandum of understanding and will include an assurance from the external agency that it complies with the laws and rules governing those individual agencies, including applicable federal and state laws.

2. Under what circumstances will the entity or contracted vendor *not disclose* LPR information?

The **[name of entity]**'s LPR information **will not** be:

- Sold, published, exchanged, or disclosed to commercial or private entities or individuals except as required by applicable law and to the extent authorized by the **[name of entity]**'s agreement with a commercial vendor.
- Disclosed or published without prior notice to the originating entity that such information is subject to disclosure or publication. However, the **[name of entity]** and the originating agency may agree in writing in advance that the **[name of entity]** will disclose LPR information as part of its normal operations, including disclosure to an external auditor of the LPR information.
- Disclosed on a discretionary basis unless the originating agency has provided prior written approval or unless such disclosure is otherwise authorized by the memorandum of understanding or agreement between the **[name of entity]** and the originating agency.
- Disclosed to unauthorized individuals.

[For commercial LPR vendors, the entity should consult its vendor agreement.]

3. State the entity's policy on confirming the existence or nonexistence of LPR information to individuals or agencies that are not authorized to receive the information.

The **[name of entity]** will not confirm the existence or nonexistence of LPR information to any individual or agency that would not be authorized to receive the information unless otherwise required by law.

H. Information Quality Assurance

1. What is the entity's policy for ensuring that the original LPR information is not altered, changed, or modified?

Original LPR information will not be altered, changed, or modified in order to protect the integrity of the data. Any changes will be maintained as a separate and additional record, and such record will be identified as having been modified.

2. For LPR alerts, what procedure must be followed to validate LPR information prior to law enforcement action (for example, prior to law enforcement initiating a traffic stop or investigative act, including analytics)?

Whenever a license plate reader alerts on license plate information, prior to taking any law enforcement action, officers will be required, to the fullest extent possible, to visually verify that the actual vehicle license plate information matches the license plate information used and alerted upon by the LPR system, including both alphanumeric characters of the license plate and the state of issuance; verify the current status of the plate as active through **[insert name of source, such as mobile information terminal [MDT] query, NCIC, etc.]**; and confirm whether the alert pertains to the registrant of the car or the car itself. Receipt of an LPR alert for a stolen or felony vehicle may not rise to the level of reasonable suspicion and is not sufficient probable cause to arrest without confirmation that the alert is still valid and active. If the alert is for another type of transaction, the officer will read the description of the alert and follow the appropriate action or reporting method. If an LPR alert cannot be verified both visually and for validity, then law enforcement should not act on the alert and it should be rejected.

If the officer witnesses a violation of law or other action that establishes reasonable suspicion for a stop, the officer may conduct a stop based on that reasonable suspicion. This provision shall not prevent a law enforcement officer from taking immediate action when a verifiable emergency situation exists for officer safety.

On each resulting alert, the officer is required to enter a disposition indicating the action taken or not taken on the alert.

3. **What is the entity's procedure for ensuring proper LPR equipment functionality?**

   The **[name of entity]** will perform routine maintenance, upgrades, calibration, and refreshes of all LPR equipment and components to ensure proper functionality, including the following:

   - At the beginning of a shift, officers will visually inspect the exterior cameras to ensure the lenses are clear and the cameras have not been altered in any way.
   - Designated, trained personnel shall check LPR equipment on a regular basis to ensure functionality and proper camera alignment.
   - Any equipment that falls outside expected functionality shall be removed from service until deficiencies have been corrected.
   - Officers will not attempt to disconnect, modify, or change the LPR equipment or software unless authorized to do so.
   - Damage or other malfunctions to the equipment will be reported to the **[insert position/title]**.
   - The LPR equipment and components will not be transferred to another vehicle except with the prior, written approval of the LPR Administrator.

4. **Does the entity research alleged or suspected errors and deficiencies of LPR information (or requests that the originating agency or vendor investigates)?**

   The **[name of entity]** will investigate, in a timely manner, alleged errors and deficiencies of LPR information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and deficiencies.

5. **How does the entity respond to confirmed errors or deficiencies of LPR information it has originated or received from an originating agency or vendor—for example, camera or system metadata (i.e., camera clock, location, image quality, Global Positioning System [GPS] errors)?**

   Note: When the original LPR record has been corrected, the [name of entity] should consider how prosecutors (and thus, defense counsel), who may be using the LPR record as evidence in a criminal case, are to be notified of such correction (i.e., written, electronic, other).

   The **[name of entity]** will correct, notate, delete, or refrain from using LPR information the **[name of entity]** originated and found to be erroneous or deficient. Originating agencies external to the **[name of entity]** are responsible for reviewing the quality and accuracy of the LPR information provided to the **[name of entity]** and must take reasonable steps to correct or amend the information upon learning that it is inaccurate or deficient. The **[name of entity]** will review the quality of LPR information it has received from an originating agency or vendor and will advise the appropriate point of contact, in writing or electronically, when its LPR information is alleged, suspected, or found to be erroneous or deficient.

6. **When the entity has provided erroneous or deficient LPR information to an external agency, what method is used to notify the external agency (written, telephonic, or electronic notification)?**

   Note: When the original LPR record has been corrected, the [name of entity] should consider how prosecutors (and thus, defense counsel), who may be using the LPR record as evidence in a criminal case, are to be notified of such correction (i.e., written, electronic, other).

   The **[name of entity]** will use written or electronic notification to inform recipient agencies **[or, if applicable, use the phrase "inform the consolidated system"]** when LPR information previously provided is erroneous or deficient. In addition, the **[name of entity]** will take reasonable steps to correct or amend the information provided to the external agency in order to ensure accuracy and sufficiency to the extent possible.

I. Redress

I.1 Disclosure

1. **May LPR information be provided *to a member of the public* in response to an information request, and are these circumstances described in the entity's redress policy? For this policy provision, consult with legal counsel to determine under what conditions, if any, LPR information would be disclosed to a member of the public.**

   Notes:
   - **This issue does not apply to circumstances in which an entity chooses to provide sensitive information in accordance with entity policy in response to an emergency situation or provide nonsensitive information to the public.**
   - **For those entities that withhold LPR information from public release using the privacy exemption under public records laws, Approach 1 under E.6 should be selected.**

   LPR information will be disclosed to the public in accordance with **[cite applicable public records laws]**. **[If the state law permits disclosure, revise provision to reflect this.]**

2. **If required by state statute, what is the entity's process for disclosing LPR information to an individual about whom LPR information has been collected or received, and if confirming identity of the requestor is required, is a record kept of all requests?**

   Note: If the state public (open) records act provides procedures for disclosure, corrections, appeals, and handling of complaints when LPR information is not subject to disclosure, these procedures should be summarized in the policy in lieu of using the sample language provided.

   Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity, an individual is entitled to know the existence of and to review the LPR information about him or her that has been collected or received and retained by the **[name of entity]**. If allowed by state law, the individual may obtain a copy of the LPR information for the purpose of challenging the accuracy or completeness of the information (correction). The **[name of entity]**'s response to the request for LPR information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests.

I.2 Corrections

1. **If, in accordance with state statute, the entity is subject to disclosure, what is the entity's procedure for handling individuals' requests for correction involving *LPR information the entity has disclosed and can change because it originated the information*? Is a record kept of requests for corrections?**

   If, in accordance with state law, an individual requests correction of LPR information *originating with the* **[name of entity]** that has been disclosed, the **[name of entity]**'s **[insert title of designee]** will inform the individual of the procedure for requesting corrections, including appeal rights for those requests that are denied in whole or in part. A record will be kept of all requests.

I.3 Appeals

1. **If requests for disclosure or corrections are denied, what is the entity's procedure for appeal?**

   The individual who has requested disclosure or to whom LPR information has been disclosed will be informed of the reason(s) why the **[name of entity]** or originating agency denied the request for disclosure or correction. The individual will also be informed of the procedure for appeal when the **[name of entity]** or originating agency has cited an exemption for the type of information requested or has declined to correct challenged LPR information to the satisfaction of the individual to whom the information relates.

J. Security and Maintenance

1. **What are the entity's physical, procedural, and technical safeguards for ensuring the security of LPR information?**

   Describe how the entity will protect the LPR information from compromise, such as:

   - **Unauthorized access**
   - **Modification**
   - **Theft**
   - **Sabotage (whether internal or external)**
   - **Natural or human-caused disasters**
   - **Intrusions**

   Consider procedures, practices, system protocols, use of software, information technology tools, and physical security measures.

   <u>Best Practice</u>: Reference generally accepted industry or other applicable standard(s) for security with which the entity complies (e.g., National Institute of Standards and Technology guidance).

   The **[name of entity and, if applicable, the name of entity's LPR vendor]** will operate in a secure facility protected from external intrusion and will utilize secure internal and external safeguards against network intrusions. Access to **[name of entity]** LPR information from outside the facility will be allowed only over secure networks.

2. **Is the entity's LPR system in compliance with the manufacturer's recommendations or any current industry standards?**

   All LPR equipment, software, and components will be properly maintained in accordance with the manufacturer's recommendations and/or any published industry standards.

3. **What requirements exist to ensure that the LPR information will be stored in a secure format and a secure environment?**

   The **[name of entity or, if applicable, the name of entity's LPR vendor]** will store LPR information in a manner that ensures that it cannot be added to, modified, accessed, or purged except by personnel authorized to take such actions.

4. **What are the requirements of personnel authorized to have access to entity LPR information?**

   Access to **[name of entity]** LPR information will be granted only to personnel whose positions and job duties require such access and who have successfully completed a background check and training.

5. **Does the entity prohibit sharing of passwords?**

   Usernames and passwords to LPR information are not transferrable, must not be shared by **[name of entity]** personnel, and must be kept confidential.

6. **Does the entity require specific configurations of strong passwords and require the replacement of manufacturer default passwords for all Web-based system access within a specified time frame?**

   User passwords must meet the following standards **[insert rules, such as no English words and a combination of letters, numbers, and at least two symbols]**. The system administrator will ensure that all manufacturer-generated default passwords are replaced with secure passwords before Web-based interfaces of the system become operational.

7. **Does electronic access to entity LPR information identify the user? Is the identity of the user retained in the audit log?**

   Queries made to the **[name of entity]**'s LPR information will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit.

8. **Is a log kept of accessed and disseminated entity-owned LPR information, and is an audit trail maintained? Refer to Section L.2, Accountability, for more information on audit logs.**

   The **[name of entity]** will maintain an audit trail of accessed, requested, or disseminated **[name of entity]**-held LPR information. An audit trail will be kept for a minimum of **[specify the retention period for your jurisdiction/entity for this type of request]** of requests for access to LPR information for specific purposes and of what LPR information is disseminated to each individual in response to the request. Audit logs will include:

   - The name and agency of the law enforcement user.
   - The date and time of access.
   - The specific information accessed.
   - The modification or deletion, if any, of the LPR information.
   - The authorized law enforcement or public safety justification for access, including a relevant case number if available. **[Note: The justification should be consistent with Section E.]**

9. **Are risk and vulnerability assessments (if maintained) stored separately from publicly available data?**

   To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

10. **What are the entity's procedures for adhering to information breach notification laws or policies?**

    Best Practice: Provide prompt notification to originating agencies when LPR information they provided to the entity has been the subject of a suspected or confirmed information breach.

    Option 1: State Information Breach Law

    The **[name of entity]** will follow the information breach notification guidance set forth in **[cite to applicable law]**. **Additional Best Practice Sample Language: [To the extent required by the (state) information breach notification law]** The **[name of entity]** will immediately notify the originating agency from which the **[name of entity]** received personal information of a suspected or confirmed breach of such information.

    Option 2: No State Information Breach Law

    A: No State Information Breach Law but the Entity Follows Guidance From the Office of Management and Budget (OMB)
    The **[name of entity]** will follow the information breach notification guidance set forth in OMB Memorandum M-07-16 (May 2007), available at http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf.

    B: Entity Adheres to the Following Policy
    [If there is no applicable state information breach notification law.] The **[name of entity]** will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the individual. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or take any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

K. Information Retention and Purging

1. **What is the entity's policy regarding retention and purging of LPR information? Reference laws, if applicable. If information is stored in multiple repositories (mobile information computer [MDC]/laptops, servers, cameras, etc.), identify each repository and its associated retention period. Agencies vary in their LPR information retention policies based in part on their strategic and tactical objectives in using the technology and the specific laws and regulations of their jurisdictions.**

   All LPR information contained within the **[name of entity]**'s LPR system will be stored for a period not to exceed **[insert a time frame]**. After **[insert time period]**, the information will be automatically purged (i.e., permanently removed from the system).

   [Entities may want to consider different retention periods for LPR information based on the legitimate law enforcement purpose for retaining the record. The following are examples.]

- **When LPR information is used for short-term situational awareness surveillance, the [name of entity] will purge information on nonviolators within [insert time period]. However, with respect to the retention of LPR information relating to First Amendment-protected events (e.g., mass gatherings), the [name of entity] limits the retention of LPR information to [insert time period].**
  Note: In accordance with *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies*,[6] "[a]gencies should limit the retention of information as much as possible to avoid the perception of maintaining files on groups or persons who engage in protected First Amendment activities."
- **For records retained locally on an MDC (and/or back-end servers), the [name of entity] will purge information within [insert time period].**

[The retention decision focuses on the LPR record as a whole. The individual components of the LPR record should not have different retention periods.]

This retention policy applies only to the LPR information contained in the **[name of entity]**'s LPR system itself. Once LPR information is downloaded by **[name of entity]** personnel and incorporated into a criminal intelligence record or an investigative case file, the LPR information is then considered intelligence or investigative information and the laws, regulations, and policies applicable to that type of information or intelligence govern its use.

If the LPR record has become or there is reason to believe that it will become evidence, including evidence that tends to inculpate or exculpate a suspect, in a specific criminal or other law enforcement investigation or action, the following provisions apply:

a. In those circumstances in which an LPR record is identified as having evidentiary value, the LPR **[insert Administrator or other title]** or designee will review the facts of the specific case and determine whether the information should be retained beyond the established retention period. If it is determined that it is reasonable to believe the information has evidentiary value, the LPR **[insert Administrator or other title]** will authorize the transfer of the applicable record from the LPR system server to **[insert appropriate response; for example, "the entity's case management system" or "a form of digital storage media (CD, DVD, etc.) or other portable storage device"]**.
b. Agencies requiring LPR records to be retained by the **[name of entity]** beyond the established retention period may make a formal, written request to the **[name of entity]** to extend retention. Each request must specify the need for extended retention, the circumstances surrounding the request, the requesting agency's case number, and a specific point of contact within the requesting agency. The **[name of entity]** reserves the right to grant or deny agency requests based on the information provided.

The **[name of entity]** retains the right to remove LPR information earlier than the retention period, based on limitations of information storage requirements and subject to applicable statutory disclosure mandates. Early removal, however, will not be used as a means for intentionally interfering with a lawful complaint or a public records request. The retention period may be modified at any time by the **[name of entity]**, subject to applicable legal requirements.

L. Accountability and Enforcement

L.1 Transparency

1. Is the entity's LPR policy available to the public?

The **[name of entity]** will be open with the public in regard to LPR information collection, receipt, access, use, dissemination, retention, and purging practices. The **[name of entity]**'s LPR policy will be made available in printed copy upon request and posted prominently on the **[name of entity]**'s Web site **[or Web page]** at **[insert Web address]**.

2. Does the entity have a point of contact for handling inquiries or complaints?

The **[name of entity]**'s **[Privacy Officer, LPR Administrator, or other position title]** will be responsible for receiving and responding to inquiries and complaints about incorrect information or privacy, civil rights, and civil liberties protections in the LPR information system maintained or accessed by the **[name of entity]**. The **[Privacy Officer, LPR Administrator, or other position title]** may be contacted at **[insert mailing address or e-mail address]**.

[6] Ibid. at 22–23.

L.2 Accountability

1. **What procedures and practices does the entity follow to enable evaluation of user compliance with system requirements, the entity's LPR policy, and applicable law?**

   The **[name of entity]** will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this LPR policy and applicable law. This will include logging access to LPR information and periodic random auditing of these systems, so as not to establish a discernable pattern that may influence users' actions. These audits will be mandated at least **[insert quarterly, semiannually, annually, or other time period]**, and a record of the audits will be maintained by the **[Privacy Officer, LPR Administrator, or title of designee]** of the **[name of entity]**. Audits may be completed by an independent third party or a designated representative of the **[name of entity]**.

   Appropriate elements of this audit process and key audit outcomes will be compiled into a report and may be provided to command staff and oversight entities or governance boards.[7]

   [Entities may also release the results of the audit to the public, pursuant to law or as a matter of discretion. Under these circumstances, consider the following options.]

   Option 1: The **[name of entity]** will provide, at minimum, an overview to the public to enhance transparency with respect to privacy, civil rights, and civil liberties protections built into the **[name of entity]**'s operations.

   Option 2: The **[name of entity]** will also release to the public the full audit, with redactions as necessary to protect the privacy of any individual or group, if appropriate and consistent with jurisdictional requirements.

2. **Does the entity have a mechanism for users or other personnel to report errors and suspected or confirmed violations of LPR policies?**

   The **[name of entity]**'s personnel or other authorized users shall report errors and suspected or confirmed violations of the **[name of entity]**'s LPR policy to the **[name of entity]**'s **[insert title of LPR Administrator]**.

3. **How often does the entity review and update the provisions contained within this LPR policy (for example, annually)?**

   The **[Privacy Officer, LPR Administrator, or other position title]** will review and update the provisions contained in this LPR policy annually and will make appropriate changes in response to changes in applicable law, technology, and/or the purpose and use of the LPR system; the audit review; and public expectations.

L.3 Enforcement

1. **What is the entity's procedure for enforcement if entity personnel, a participating agency, or an authorized user is suspected of being or has been found to be in noncompliance with the provisions of this policy?**

   If **[name of entity]** personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, receipt, access, use, dissemination, retention, and purging, the **[title of entity Director]** of the **[name of entity]** will:

   - Suspend or discontinue access to information by the **[name of entity]** entity personnel, the participating agency, or the authorized user;
   - Apply appropriate disciplinary or administrative actions or sanctions;
   - If the authorized user is from an agency external to the **[name of entity]**, request that the user's employer initiate disciplinary proceedings to enforce the policy's provisions; and/or
   - Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

[7] *Privacy, Civil Rights, and Civil Liberties Audit Guidance for the State, Local, Tribal, and Territorial Intelligence Component*, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/181/Privacy--Civil-Rights--and-Civil-Liberties-Audit-Guidance-for-the-State--Local--Tribal--and-Territorial-Intelligence-Component.

2. **What is the entity's policy with regard to the qualifications and number of participating agency personnel authorized to access entity LPR information, and what additional sanctions are available for violations of the entity's LPR policy?**

   The **[name of entity]** reserves the right to establish the qualifications and number of personnel having access to **[name of entity]** LPR information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating this LPR policy.

M. Training

1. **What personnel does the entity require to participate in training programs, before access to entity LPR information is granted, regarding implementation of and adherence to this LPR policy?**

   Before access to **[name of entity]** LPR information is authorized, the **[name of entity]** will require the following individuals to participate in training regarding implementation of and adherence to this LPR policy:

   - All authorized **[name of entity]** personnel.
   - All authorized participating agency personnel.
   - All authorized personnel providing information technology services to the **[name of entity]**.

2. **What is covered by the entity's LPR training program (for example, purpose of the LPR policy, substance and intent of the provisions of the LPR policy, impact of infractions, and possible penalties for violations)?**

   The **[name of entity]**'s LPR policy training program will cover:

   - Purposes of the LPR policy.
   - Substance and intent of the provisions of this LPR policy and any revisions thereto relating to collection, receipt, access, use, dissemination, retention, and purging of the **[name of entity]**'s LPR information and the privacy, civil rights, and civil liberties protections on the use of the technology and the information collected or received.
   - Appropriate procedures relating to license plate image quality and mitigating the risks associated with a possible misread by the LPR system.
   - LPR verification process for law enforcement alerts.
   - Originating and participating agency responsibilities and obligations under applicable federal, state, or local law and policy.
   - How to implement the LPR policy in the day-to-day work of the user, whether a paper or systems user.
   - Mechanisms for reporting violations of **[name of entity]** LPR policy provisions.
   - The nature and possible penalties for LPR policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

(This Page Intentionally Left Blank)

Appendix A—Glossary of Terms and Definitions

The following is a list of primary terms and definitions used throughout this template. These terms are also useful in drafting the definitions section of the entity's LPR policy.

Access—Information access is being able to get to (usually having permission to use) particular information on a computer. Information access is usually specified as edit, enter, modify, or read-only and read/write access. Web access means having a connection to the Internet through an access provider or an online service provider.

Access Control—The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role- or user-based.

Acquisition—The means by which an entity obtains LPR information through the exercise of its authorities.

Agency—A participating agency that accesses, contributes, and/or shares information in the **[name of entity]**'s justice information system.

Aggregation of LPR Data—Refers to information that becomes part of a case file. It is also called "used data," and it shall be compliant with applicable laws and regulations.[8]

Alert—A visual and/or auditory notice that is triggered when the LPR system receives a potential "hit" on a license plate.

Audit Trail—A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—What commands were issued to the system? What records and files were accessed or modified?

Audit trails are a fundamental part of computer security and system user accountability and are used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication—The process of validating the credentials of an individual, a computer process, or a device. Authentication requires that the individual, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of usernames and passwords.

Authorization—The process of granting an individual, a computer process, or device access to certain information, services, or functionality. Authorization is derived from the identity of the individual, a computer process, or a device requesting access that is verified through authentication. See Authentication.

[8] Automated License Plate Recognition (ALPR), General Order 17.102, Tempe Police Department, Arizona, 12-13-2003.

Automatic License Plate Reader (ALPR)—ALPR systems comprise high-speed cameras mounted at a fixed location or on a mobile patrol vehicle (see Fixed LPR, Mobile LPR, and Portable LPR definitions) that function to:

- Automatically capture an image of a vehicle's license plate.
- Transform that image into alphanumeric characters using optical character recognition or similar software.
- Compare the plate number acquired to one or more databases of vehicles of interest to law enforcement and other agencies.
- Alert officers when a vehicle of interest has been observed.

The automated capture, use, and comparison of vehicle license plates typically occur within seconds, alerting officers when a wanted plate is observed.[9] A standard LPR record contains, at a minimum, an OCR interpretation of the captured image, a photo of the license plate and a contextual photo of an area surrounding the plate that could range from a few inches to a larger area around the entire vehicle; the geographic coordinates of where the image was captured; the date and time of the recording; and the specific camera/unit that captured the image. Retained LPR information does not include specific identification of individuals.

The following are other names used for this technology:

- Automated license plate recognition (ALPR)
- Automatic license plate recognition (ALPR)
- Automatic number plate recognition (ANPR)
- Automatic vehicle identification (AVI)
- Car plate recognition (CPR)
- License plate recognition (LPR)
- Mobile license plate reader (MLPR)
- Vehicle license plate recognition (VLPR)

Be On the Lookout (BOLO)—Refers to an indication by a law enforcement agency that there is an articulable and specific law enforcement reason to identify or locate a particular vehicle or, in the case of a post-scan BOLO, that there is an articulable and specific reason to ascertain the past location(s) of a particular vehicle.

BOLO List—Also known as a hot list, a compilation of one or more license plates or partial license plates of a vehicle or vehicles for which a BOLO situation exists that is programmed into an LPR so that the device will alert if it captures the image of a license plate that matches a license plate included on the BOLO list. The term also includes a compilation of one or more license plates or partial license plates that is compared against stored license plate information that had previously been scanned and collected by an LPR, including scanned license plate information that is stored in a separate information storage device or system. See Hot List.

Civil Liberties—According to the U.S. Department of Justice's Global Justice Information Sharing Initiative, the term "civil liberties" refers to fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals.

Civil Rights—The term "civil rights" refers to those rights and privileges of citizenship and equal protection that the state is constitutionally bound to guarantee all citizens regardless of race, ethnicity, religion, gender, national origin, religion, sexual orientation, gender identity, or other characteristics unrelated to the worth of the individual. Protection of civil rights imposes an affirmative obligation upon government to promote equal protection under the law. Generally, the term "civil rights" involves positive (or affirmative) government action to protect against infringement, while the term "civil liberties" involves restrictions on government.[10]

Collect—For purposes of this document, "gather" and "collect" mean the same thing.

Confidentiality—Refers to the obligations of individuals and entities to appropriately use information and data under their control once they have been disclosed to them and in accordance with applicable data security laws and policies. See Privacy.

Credentials—Information that includes identification and proof of identification that are used to gain access to local and network resources. Examples of credentials are usernames, passwords, smart cards, and certificates.

Criminal Activity—A behavior, an action, or an omission that is punishable by criminal law.[11]

Criminal Case Support—Those administrative or analytic activities that provide relevant information to law enforcement personnel regarding the investigation of specific criminal activities or trends or specific subject(s) of criminal investigations.[12]

Data Breach—The unintentional release of secure information to an untrusted environment. Your response to a data breach may be addressed in state law or agency policy. This may include incidents such as:

- Theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted.

[9] Automated License Plate Recognition, "About ALPR" Web page, International Association of Chiefs of Police, http://www.iacp.org/ALPR-About.

[10] Civil Rights and Civil Liberties Protections Guidance (September 2008). The definition of "civil rights" is a modified version of the definition contained in the *National Criminal Intelligence Sharing Plan* (NCISP), at pp. 5–6.

[11] *License Plate Reader—Standard Operating Procedure*, Appendix—Definitions, Maryland Coordination and Analysis Center, www.mcac.maryland.gov/resources/LPR/LPR-SOP.html.

[12] Ibid.

- Posting such information on the Internet.
- Unauthorized employee access to certain information.
- Moving such information to a computer otherwise accessible from the Internet without proper information security precautions.
- Intentional or unintentional transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail.
- Transfer of such information to the information systems of a possibly hostile entity or environment where it may be exposed to more intensive decryption techniques.

Direct LPR Collection—The entity is the owner of the LPR equipment that captures LPR information.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, an entity, or an organization outside the entity that collected it.

Dissemination—See Disclosure.

Electronically Maintained—Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, compact disc optical media, or cloud technologies.

Electronically Transmitted—Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, or transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, or faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voicemail.

Entity—The **[name of entity],** which is the subject and owner of the LPR policy.

Fair Information Practice Principles—The Fair Information Practice Principles (FIPPs) are a set of internationally recognized principles that inform information privacy policies both within government and the private sector. Although specific articulations of the FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into information privacy laws, policies, and governance documents around the world. They provide a straightforward description of underlying privacy and information exchange principles and a simple framework for the legal use that needs to be done regarding the impact of an LPR system on individual privacy. Some of the individual principles, such as Principle 7, may not apply in all instances of an integrated justice system.

The eight principles are:

1. Collection Limitation/Data Minimization
2. Data Quality/Integrity (See definition.)
3. Purpose Specification
4. Use Limitation
5. Security Safeguards (See definition.)
6. Openness/Transparency
7. Individual Participation
8. Accountability/Audit

See Appendix B for one description of how the U.S. Department of Homeland Security applies these principles.

Firewall—A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

Fixed LPR—LPR cameras that are permanently affixed to a structure, such as a pole, a traffic barrier, or a bridge.

Hit—A read matched to a plate which has previously been registered on an agency's "hot list" of vehicle plates related to stolen vehicles, wanted vehicles, or other factors supporting investigation or which has been manually registered by a user for further investigation.

Hot List—A file that contains the license plate numbers of stolen vehicles; stolen license plates; AMBER, SILVER, or other law enforcement alerts; lists of license plate numbers known to be associated with specific individuals, such as wanted individuals or missing individuals (e.g., wanted for homicide, rape, robbery, child abduction); or terrorist watch lists. The Motor Vehicle Administration also provides suspended or revoked registrations. A hot list is routinely updated but does not rely on real-time communications with state or federal information sources. LPR hot lists are compiled to serve agency-specified needs. Manual entry may be available, allowing additions for specific license plates. The hot list is essential to LPR systems, as it is required in order to notify law enforcement that a vehicle on the list is near an LPR camera.[13] See Be On the Lookout.

Identification—A process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that uniquely differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or a collection of data, such as a given and family name, date of birth, and address. An organization's identification process consists of the acquisition of the relevant identifying information.

Information—Inert symbols, signs, descriptions, or measures; elements of information. Includes any information about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement entities can be categorized into four general areas: general data, including

[13] Ibid.

investigative information; tips and leads data; suspicious activity reports; and criminal intelligence information.

Information Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, receipt, use, dissemination, retention, purging, and protection of information.

Information Quality (IQ)—Refers to various aspects of the information; the accuracy and validity of the actual values of the data, information structure, and database/information repository design. Traditionally, the basic elements of IQ have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, IQ is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy. This concept is also addressed as one of the Fair Information Practice Principles, Data Quality/Integrity. See Appendix B for a full set of the FIPPs.

Information Sharing Environment (ISE)—In accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, the Information Sharing Environment (ISE) is a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of state, local, tribal, and territorial (SLTT) agencies; federal agencies; and the private sector to facilitate terrorism-related information sharing, access, and collaboration.

Invasion of Privacy—Intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. See also Right to Privacy.

Least Privilege Administration—A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform.

Legitimate Law Enforcement Purpose—The investigation, detection of a crime, or a violation of the law and/or the operation of terrorist or missing or endangered individual searches or alerts.[14]

Linkable Information—Information about or related to an individual for whom there is a possibility of logical association with other information about that individual.[15]

Linked Information—Information about or related to an individual that is logically associated with other information about that individual.[16]

Logs—A necessary part of an adequate security system because they are needed to ensure that information is properly tracked and that only authorized individuals are getting access to the data. See also Audit Trail.

LPR—Refer to Automatic License Plate Reader (ALPR).

LPR Information[17]—The images and the metadata associated with them are the primary forms of information collected by an LPR system. Information files typically contain the following information:

- Black-and-white plate image
- Contextual color image
- Electronically readable format of plate
- Alphanumeric characters of license plate numbers
- Location and GPS coordinates
- Time and date of image capture
- Camera identification

LPR System—A set of equipment used to capture license plate images and associated data. The equipment may include the following:

- One or more LPR cameras
- Processor for converting the images to text
- Optical Character Recognition (OCR) engine optimized for reading license plates
- GPS receiver
- Brackets or mounting hardware
- Connect cables

See also Automatic License Plate Reader, Fixed LPR, Mobile LPR, or Portable LPR.

Maintenance of Information—Applies to all forms of information storage. This includes electronic systems (for example, databases) and nonelectronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves that organization's purpose.

Mobile LPR—Intended for use in a moving motor vehicle (i.e., camera is moving) and typically mounted semipermanently to a marked patrol vehicle. A mobile LPR typically includes one to four cameras and the configuration is set at the discretion of the contributing agency based on driving patterns and street configurations.

Need to Know—As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counterterrorism activity or other authorized government duty, such as to further an investigation or meet another law enforcement requirement.

[14] Ibid.
[15] Automated License Plate Recognition (ALPR), General Order 17.102, Tempe Police Department, Arizona, 12-13-2003.
[16] Ibid.
[17] Automated License Plate Recognition (ALPR), General Order 17.102, Tempe Police Department, Arizona, 12-13-2003.

Nonencounter Alert—Refers to an immediate alert in which the officer operating the LPR is instructed to notify the agency that put out the alert without initiating an investigative detention of the subject vehicle or otherwise revealing to the occupant(s) of that vehicle that its location has been detected or that it is the subject of law enforcement attention.

Nonrelevant Information—Information regarding a vehicle's location—particularly when collected over an extended period of time—may be misused to infer additional information about an individual that is not relevant to police purposes and potentially sensitive for the individual. Such inferences may include but are not limited to nonrelevant personal relationships, marital fidelity, religious observance, and political activities such as attending rallies or vote canvassing. By precisely and proportionally limiting access to LPR information, the risks of such misuse can be reduced and the likelihood of inferring protected/nonrelevant character attributions can be minimized. In addition, by ensuring that information lawfully collected but determined to be nonrelevant is purged upon classification as nonrelevant, entities further mitigate the privacy risks.

Participating Entity—A public safety or law enforcement agency that owns and/or operates LPR cameras, contributes information to the LPR system, and is authorized to access or receive entity LPR information.

Permissions—Authorization to perform operations associated with a specific shared resource, such as a file, a directory, or a printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personal Information—Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in criminal activity, including terrorism. See also Personally Identifiable Information (PII).

Personally Identifiable Information (PII)—One or more pieces of information that, when considered alone, in the context of how the information is presented or gathered, or when combined with other information, are sufficient to specify a unique individual. The pieces of information can be, but are not limited to:

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).
- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, social media user name, driver's license number, financial account or credit card number and associated PIN number, Integrated Automated Fingerprint Identification System [IAFIS] identifier, or booking or detention system number).
- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Portable LPR—LPR cameras that are transportable and can be moved and deployed in a variety of venues as needed, such as a traffic barrel or speed radar sign.

Privacy—Refers to individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Policy—A printed, published statement that articulates the policy position of an organization on how it handles the personal information that it collects or receives and accesses or uses in the normal course of business. The policy should include information relating to the processes of information collection, receipt, access, use, dissemination, retention, and purging. It is likely to be informed by the Fair Information Practice Principles (FIPPs). The purpose of the privacy policy is to articulate that the entity will adhere to those legal requirements and entity policy determinations that enable collection, receipt, access, use, dissemination, retention, and purging of information to occur in a manner that protects personal privacy interests.

Public—Public includes:

- Any individual and any for-profit or nonprofit entity, organization, or association.
- Any governmental entity for which there is no existing specific law authorizing access to the entity's information.
- Media organizations.
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit and without distinction as to the nature or intent of those requesting information from the entity or participating entity.

Public does not include:

- Any employees of the entity or participating entity.
- People or entities, private or governmental, who assist the entity in the operation of the justice information system.
- Public entities whose authority to access information collected or received and retained by the entity is specified in law.

Public Access—Relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.

Purge—A term that is commonly used to describe methods that permanently erase and remove data from a storage space. There are many different strategies and techniques for data purging, which is often contrasted with data deletion.

Read—Digital images of license plates and associated metadata (e.g., date, time, and geographic coordinates associated with the vehicle image capture) that are captured by the LPR system.

Record—Any item, collection, or grouping of information that includes PII and is collected, received, accessed, used, disseminated, retained, and purged by or for the collecting entity or organization.

Redress—Laws, policies, and procedures that address public entity responsibilities with regard to access/disclosure and correction of information and the handling of complaints from individuals regarding *protected information* about them which is under the entity's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

Protected information includes personal information about individuals that is subject to information privacy or other legal protections by law. Protection may also be extended to organizations by center policy or state, local, tribal, or territorial law.

Retention—Refer to Storage.

Right to Know—Based on having legal authority or responsibility or pursuant to an authorized agreement, an entity or an organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, counterterrorism activity, or other authorized government duty.

Right to Privacy—The right to be left alone, in the absence of some reasonable public interest in collecting, accessing, retaining, and disseminating information about an individual's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the individual or entity violating an individual's privacy.

Role-Based Access—A type of access authorization that uses roles to determine access rights and privileges. A role is a symbolic category of users that share the same security privilege.

Scan—Refers to the process by which an LPR automatically focuses on, photographs, and converts to digital text the license plate of a vehicle that comes within range of the LPR.

Security—Refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of information for the legitimate user set, as well as promoting failure resistance in the electronic systems overall. Security safeguarding of information is a Fair Information Practice Principle. See Appendix B.

Source Entity—Refers to the entity or organizational entity that originates LPR information.

Storage—In a computer, storage is the place where information is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

Storage is frequently used to mean the devices and information connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This is probably the most common meaning in the IT industry.

In a more formal usage, storage has been divided into (1) primary storage, which holds information in memory (sometimes called random access memory, or RAM) and other "built-in" devices, such as the processor's L1 cache, and (2) secondary storage, which holds information on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more information than primary storage.

User—An entity employee or an individual representing a participating entity who is authorized to access or receive and use an entity's information and intelligence databases and resources for lawful purposes.

Appendix B—Fair Information Practice Principles (FIPPs)

The Fair Information Practice Principles (FIPPs) are a set of internationally recognized principles that inform information privacy policies within both government and the private sector.

Although specific articulations of the FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into data privacy laws, policies, and governance documents around the world. For example, the FIPPs are:

- At the core of the Privacy Act of 1974, which applies these principles to U.S. federal agencies.[18]
- Influential internationally, especially as articulated by the Organisation for Economic Co-operation and Development.
- Mirrored in many states' laws and in fusion centers' privacy policies.
- Used by numerous foreign countries and international organizations.

The following formulation of the FIPPs is used and implemented for the Information Sharing Environment (ISE) by the U.S. Department of Homeland Security (DHS).[19] For a definition of the Information Sharing Environment, refer to Appendix A, Glossary of Terms and Definitions.

1. **Purpose Specification—**Agencies should specifically articulate the authority that permits the collection of personally identifiable information (PII). The purpose(s) for which PII is collected should be specified at the time of data collection. Subsequent use of this data should be limited to the original purpose for which the PII was collected (or other purposes *compatible* with the original collection purpose).

   Implementing the Purpose Specification Principle—Agencies are bound by specific constitutional and statutory authorities that circumscribe their ability to collect PII. The following are examples of ways agencies may implement this principle:

   - Ensure that a valid lawful purpose exists and is documented for all collection of PII.
   - Include the source and authority for the data so that access restrictions can be applied.
   - Upon receipt of data containing PII from third parties, if possible, identify the purpose for which it was collected initially and limit agency use to only those uses compatible with the original purpose supporting collection.
   - Ensure that metadata or other tags are associated with the data as it is shared.
   - Institute a two-individual review and approval process to consider any Privacy Act or other legal or policy limitation before permitting use or sharing of data for purposes other than that for which it was collected.

2. **Data Quality/Integrity—**PII collected should be relevant to the purposes identified for its use and should be accurate, complete, and up to date.

[18] 5 U.S.C. § 552a.
[19] 6 U.S.C.§ 142.

Implementing the Data Quality/Integrity Principle—One important way to minimize potential downstream privacy and civil liberties concerns is to ensure that any information collected, stored, and disseminated is accurate. This includes ensuring that the information provides sufficient context for any PII. Possible approaches include:

- Properly labeling PII.
- Determining a policy for safeguarding PII if there are "mixed" databases (i.e., those databases with personal information on U.S. individuals and others, regardless of nationality).
- Instituting a source verification procedure to ensure reporting is based only on authorized data.
- Reconciling and updating PII whenever new relevant information is collected.
- Developing a protocol for ensuring data corrections are passed to those entities with which information has been shared.
- Creating a documented process for identifying and addressing situations in which data has been erroneously received, is inaccurate or has been expunged.

3. **Collection Limitation/Data Minimization—**PII should be collected only if the data is directly relevant and necessary to accomplish the specified purpose. PII should be obtained by lawful and fair means and retained only as long as is necessary to fulfill the specified purpose.

   Implementing the Collection Limitation/Data Minimization Principle—Collection limitation may be implemented by:

   - Designing a data storage system to pull data for review and then, if appropriate, automatically purging data after the specified retention period has been reached.
   - Limiting data field elements to only those that are relevant.
   - Ensuring that all distributed reports and products contain only that personal information that is relevant and necessary (nothing extraneous or superfluous).
   - Ensuring that all shared information with PII meets required thresholds for sharing, such as reasonable suspicion.

4. **Use Limitation—**PII should not be disclosed, made available, or otherwise used for purposes other than those specified except (a) with the consent of the individual or (b) by the authority of law.

   Implementing the Use Limitation Principle—Sharing information should be tempered by adherence to key principles, such as "authorized access." Use limitation may be implemented by:

   - Limiting users of data to those with credential-based access.
   - Requiring that justifications be entered and logs maintained for all queries with sensitive PII and that an internal review process of those logs takes place at specified intervals.
   - Requiring senior analysts to review all reports that use PII before dissemination to ensure (a) that PII is relevant and necessary and (b) that the recipient is authorized to receive the information in the performance of an authorized activity.
   - Prior to sharing information, verify that partners have a lawful purpose for requesting information.
   - Creating multiple use-based distribution lists and restricting distribution to those authorized to receive the information.

5. **Security/Safeguards—**Agencies should institute reasonable security safeguards to protect PII against loss, unauthorized access, destruction, misuse, modification, or disclosure.

   Implementing the Security/Safeguards Principle—This principle can be implemented by:

   - Maintaining up-to-date technology for network security.
   - Ensuring that access to data systems requires that users meet certain training and/or vetting standards and that such access is documented and auditable.
   - Ensuring that physical security measures are in place, such as requiring an identification card, credentials, and/or passcode for data access; disabling computers' USB ports; and implementing firewalls to prevent access to commercial e-mail or messaging services.
   - Implementing a protocol with technical and manual safeguards to ensure the accuracy and completeness of data system purges when records are deleted at the end of their retention period.
   - Ensuring that data system purge protocols include complete record deletion on all backup systems.
   - Transitioning older repositories into more modern systems to improve access controls.
   - Masking data so that it is viewable only to authorized users.

- Maintaining an audit log to record when information is accessed and by whom for review by senior staff at specified intervals.
- Requiring authorized users to sign nondisclosure agreements.

6. **Accountability/Audit—**Agency personnel and contractors are accountable for complying with measures implementing the FIPPs, for providing training to all employees and contractors who use PII, and for auditing the actual use and storage of PII.

   Implementing the Accountability/Audit Principle—Strong policies must not only be in place but also be effectively implemented. Accountability can be demonstrated by:

   - Ensuring that upon entry for duty, all staff take an oath to adhere to the privacy and civil liberties protections articulated in the center's or host agency's mission, core values statements, other key documents, and/or the U.S. Constitution.
   - Conducting effective orientation and periodic refresher training, including privacy, civil rights, and civil liberties protections, for all individuals handling PII.
   - Tailoring training to specific job functions, database access, or data source/storage requirements.
   - Conducting regular audits of all systems in which records are kept to ensure compliance with privacy, civil rights, and civil liberties policies and all legal requirements.
   - Following a privacy incident, establishing a handling procedure for any data breaches or policy violations.
   - Denying database access to individuals until they have completed mandatory systems access training (including training for handling of PII), show a mission need for access, and have any necessary clearances.
   - Developing targeted and consistent corrective actions whenever noncompliance is found.

7. **Openness/Transparency—**To the extent feasible, agencies should be open about developments, practices, and policies with respect to the collection, use, dissemination, and maintenance of PII. Agencies should publish information about policies in this area, including the privacy, civil rights, and civil liberties policy, and contact information for data corrections and complaints.

   Implementing the Openness/Transparency Principle—Agencies can implement the Openness/Transparency principle by:

   - Providing reports to an internal or external oversight body concerned with privacy, civil rights, and civil liberties issues, including privacy, civil rights, and civil liberties audit results.
   - Publishing the privacy, civil rights, and civil liberties policy and redress procedures.
   - Meeting with community groups through initiatives or other opportunities to explain the agency's mission and privacy, civil rights, and civil liberties protections.
   - Responding in the fullest way possible to freedom of information and/or sunshine requests and fully explaining any denial of information requests from the public.
   - Conducting and publishing Privacy Impact Assessments (PIAs) in advance of implementing any new technologies that affect PII thereby demonstrating that privacy, civil rights, and civil liberties issues have been considered and addressed.

8. **Individual Participation—**To the extent practicable, involve the individual in the process of using PII and seek individual consent for the collection, use, dissemination, and maintenance of PII. Agencies should also provide mechanisms for appropriate access, correction, and redress regarding the agency's use of PII.

   Implementing the Individual Participation Principle—To the extent appropriate, agencies can implement the Individual Participation principle by:

   - Collecting information directly from the individual, to the extent possible and practical.
   - Providing the individual with the ability to find out whether a project maintains a record relating to him or her and, if not (i.e., access and/or correction is denied), then providing the individual with notice as to why the denial was made and how to challenge such a denial.
   - Putting in place a mechanism by which an individual is able to prevent information about him or her that was obtained for one purpose from being used for other purposes without his or her knowledge.

(This Page Intentionally Left Blank)

Appendix C—Listing of Federal Laws

The U.S. Constitution is known as the primary authority that applies to federal as well as state, local, tribal, and territorial (SLTT) entities. State constitutions cannot provide a lower level of privacy and other civil liberties protection than that established by the U.S. Constitution, but states can broaden constitutional rights guaranteed by their own constitutions.

Civil liberties protections are primarily founded in the Bill of Rights. They include the basic freedoms, such as free speech, assembly, and religion; freedom from unreasonable search and seizure; due process; etc. Statutory civil rights protections in the U.S. Constitution may, in addition, directly govern state action. These include the Civil Rights Act of 1964, as amended; the Rehabilitation Act of 1973; the Equal Educational Opportunities Act of 1974; the Americans with Disabilities Act; the Fair Housing Act; the Voting Rights Act of 1965; and the Civil Rights of Institutionalized Individuals Act.

While SLTT entities may not be generally bound directly by most statutory federal privacy and other civil liberties protection laws in the LPR information collection sharing context, compliance may be required **indirectly** by funding conditions (e.g., Title VI of the Civil Rights Act of 1964), operation of the Commerce Clause of the U.S. Constitution, or a binding agreement between a federal agency and an SLTT entity (e.g., a memorandum of agreement or a memorandum of understanding). When relevant or possibly relevant, entities/agencies are advised to list laws, regulations, and policies within their LPR policy, noting those that may potentially affect the sharing of information.

The development of an LPR policy is primarily designed for entity personnel and authorized users to ensure that they are aware of the legal and privacy framework within which they and the entity must operate. If the applicability and requirements of various laws, regulations, or sharing agreements are not spelled out or referenced in an entity's LPR policy, staff and user accountability is greatly diminished, mistakes are made, privacy violations occur, and the public's (and other agencies') confidence in the ability of the entity to protect LPR information is compromised. When staff members know the rules through sound policy and procedure communicated through ongoing training activity, LPR information sharing is enhanced.

"At the time of this writing there are no federal laws that explicitly govern or limit the use of ALPR technology or taking photographs of things that are plainly visible from public spaces by law enforcement agencies."[20] Many jurisdictions are actively developing or considering legislation that will authorize, limit, and/or restrict the use of ALPR systems and the information they generate. Some examples of specific legislative proposals and legislation that have passed include:

- **Arkansas:** Act 849 of 2015, To Allow the Arkansas Highway Police Division of the Arkansas State Highway and Transportation Department to Utilize the Automatic License Plate Reader System, and Act 1491 of 2013, To Regulate the Use of Automatic License Plate Reader Systems
- **California:** Senate Bill 34 of 2015, Automatic License Plate Recognition Systems: Use of Data
- **Colorado:** House Bill 14-1152, Concerning Passive Surveillance Records of Governmental Entities
- **Florida:** Senate Bill 226
- **Illinois:** SB 1351 - Automated License Plate Recognition System Information Act (2/18/15)
- **Tennessee:** Senate Bill 1664

[20] Automated License Plate Reader Frequently Asked Questions Web page, IACP, www.iacp.org/ALPR-FAQs.

- **Utah:** Senate Bill 196, License Plate Reader Amendments (2013); Senate Bill 222 (LPR amendment; and Senate Bill 51 (LPR Amendment)
- **Maine:** Title 29 Section 2117
- **Maryland:** Senate Bill 699, Automatic License Plate Readers and Captured Plate Data – Authorized Uses
- **Minnesota:** Senate Bill 86, A bill for an act relating to data practices; classifying data related to automated license plate readers and requiring a governing policy; requiring a log of use; requiring data to be destroyed in certain circumstances; and requiring a report
- **North Carolina:** Senate Bill 182, An Act to Regulate the Use of Automatic License Plate Reader Systems
- **Vermont:** Senate Bill 18, An Act Relating to Privacy Protection[21]

The following are synopses of primary federal laws that an entity should review and, where appropriate, consider citing in an LPR policy to protect the LPR record and any personally identifiable information later associated with the LPR record. As LPR information may be incorporated as one piece of information into a larger case file, the following federal laws may be applicable. The list is arranged in alphabetical order by popular name.

1. **Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721—Prohibition on Release and Use of Certain Personal Information from State Motor Vehicle Records—**Collected LPR information contains no personally identifiable information that may be used to connect a license plate detection to an individual. It is only with permissible purpose that law enforcement may make this connect (using other systems) and this access is governed by the Driver's Privacy Protection Act of 1994.

2. **E-Government Act of 2002, Public Law 107–347, 208, 116 Stat. 2899 (2002**)**—**This act requires federal agencies to perform Privacy Impact Assessments (PIAs) for new information technologies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing information technology that manages information in identifiable form. A PIA is an evaluation of how information in identifiable form is collected, stored, protected, shared, and managed. The purpose of a PIA is to demonstrate that system owners and developers have incorporated privacy protections throughout the entire life cycle of a system. The act requires an agency to make PIAs publicly available, except when an agency in its discretion determines publication of the PIA would raise security concerns or reveal classified (i.e., national security) information or sensitive (e.g., potentially damaging to a nation interest, law enforcement effort, or competitive business interest contained in the assessment) information. Although this act does not apply to SLTT partners, this tool is useful for identifying and mitigating privacy risks and for notifying the public what PII the SLTT agency is collecting, why PII is being collected, and how the PII will be collected, used, accessed, shared, safeguarded, and stored.

3. **Federal Civil Rights Laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983—**This is a federal statute that allows an individual to sue public officials in federal court for violations of the individual's civil rights. Civil rights include the Fourth Amendment's prohibitions against unreasonable search and seizure, violations of privacy rights, and violations of the right to freedom of religion, free speech, and free association. It serves as a deterrent to unlawful collection, use, or sharing of information rather than providing specific authority or a prohibition to the collection, use, or sharing of information.

4. **Federal Driver's Privacy Protection Act (DPPA), 18 USC § 2721-2725**—Restricts access and prohibits the release of personal information from state motor vehicle records to ensure the privacy of citizens.

5. **Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301**—This chapter contains the laws governing disposal of records made or received by a federal agency in the normal course of business. It discusses purging procedures and notices, if required, and the role of the federal archivist. The law applies only to federal agencies, but there may be similar state or local laws applicable to state and local agencies.

6. **Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552—**The federal FOIA, enacted in 1966, provides access to federal agency records or information. It does not, however, allow access to state or local government records. Nearly all states have their own public access statutes that provide access to state- and local-agency records. The interaction of federal and state FOIA laws can create complex issues. Federal statutes, in essence, provide a baseline of legal protections for individuals. While state legislatures may pass laws to supplement these federal guidelines, state laws that interfere with or are contrary to a federal law are preempted. By virtue of the Supremacy Clause of the U.S. Constitution (Article VI, Clause 2), federal law may restrict access to records otherwise available pursuant to a state's FOIA by requiring that certain

[21] For more information on state legislation that was introduced/considered regarding LPRs, refer to the National Conference of State Legislatures, ALPR State Legislation page, www.ncsl.org/research/telecommunications-and-information-technology/2014-state-legislation-related-to-automated-license-plate-recognition-information.aspx; for further information, see ALPR Policy and Privacy, IACP, www.iacp.org/ALPR-Policy.

information be kept confidential. Thus, federal confidentiality requirements may supersede a state FOIA statute mandating public disclosure of a record, but only when there is a specific federal statute (other than the federal FOIA) that mandates the records be kept confidential. In short, records may be available under one FOIA statute but not pursuant to another.

7. **Indian Civil Rights Act of 1968, 25 U.S.C. § 1301 et seq., United States Code, Title 25, Chapter 15, Subchapter I—**This act contains definitions of relevant terms and extends certain constitutional rights to Indian tribes exercising powers of self-government.

8. **National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993), 107 Stat. 2490—**In each state, an authorized criminal justice agency of the state shall report child abuse crime information to or index child abuse crime information in the national criminal history background check system. A criminal justice agency can satisfy the requirement by reporting or indexing all felony and serious misdemeanor arrests and dispositions. The U.S. Attorney General (AG) is required to publish an annual statistical summary of child abuse crimes. The act requires that 80 percent of final dispositions be entered in the state databases by December 1998, with steps being taken toward 100 percent entry.

   A 1994 amendment required that the AG—in consultation with federal, state, and local officials, including officials responsible for criminal history record systems, and representatives of public and private care organizations and health, legal, and social welfare organizations—shall develop guidelines for the adoption of appropriate safeguards by care providers and by the state for protecting children, the elderly, and individuals with disabilities from abuse.

9. **NIST Special Publication 800-53 (Appendix J) *Security and Privacy Controls for Federal Information Systems and Organizations*—**Federal agencies are required to ensure that privacy protections are incorporated into information security planning. To that end, SP 800-53 Rev. 4 features eight families of privacy controls that are based on the FIPPs. The proliferation of social media, Smart Grid, mobile, and cloud computing as well as the transition from structured to unstructured information and metadata environments have added significant complexities and challenges for federal organizations in safeguarding privacy. These challenges extend well beyond the traditional information technology security view of protecting privacy, which focused primarily on ensuring confidentiality. The use of these standardized privacy controls will provide a more disciplined and structured approach for satisfying federal privacy requirements and demonstrating compliance with those requirements. Like their federal partners, SLTT agencies may use the privacy controls when evaluating their systems, processes, and programs.

10. **Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a—**The Privacy Act establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals, which is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by using the name of the individual or some identifier assigned to that individual. The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual, unless the disclosure is pursuant to one of 12 statutory exceptions. The act also provides individuals with a means by which to seek access to and amendment of their records and sets agency record-keeping requirements. In addition, the Privacy Act requires that agencies give the public notice of their systems of records by publication in the *Federal Register*.

11. **Protection of Sensitive Agency Information, Office of Management and Budget Memorandum M-06-16 (June 2006)—**This memorandum provides a security checklist from the National Institute of Standards and Technology (NIST) to protect remote information removed from or accessed from outside an agency's physical location specific to personally identifiable information (PII). The NIST checklist requires that agencies verify PII in need of protection, confirm the adequacy of organization policy surrounding PII protection, and implement any necessary protections for PII transported or stored off-site or accessed remotely. In addition to the NIST checklist, the memorandum recommends implementing information encryption on all mobile devices, allowing remote access only with two-factor authentication, using timeout functions on devices, and logging all computer-readable information extracts from databases with sensitive information, while verifying that each extract has either been erased within 90 days or its use is still required.

12. **Safeguarding Against and Responding to the Breach of Personally Identifiable Information, OMB Memorandum M-07-16 (May 2007)—**This memorandum applies to federal agency-held information and information systems, requiring development and implementation of a breach notification policy applicable to personally identifiable information in the possession of the agency. Development of a breach notification policy includes a review of existing privacy and security requirements, development of requirements for incident reporting and handling, and procedures for internal and external notification. SLTT agencies that are not subject to an existing breach notification law or policy may use the federal requirements as a template for developing their own breach notification policy.

13. **U.S. Constitution, First, Fourth, Fifth, Sixth, and Fourteenth Amendments—**The Bill of Rights establishes minimum standards for the protection of the

civil rights and civil liberties of Americans. The First Amendment protects religious freedom, speech, the press, the right to peaceably assemble, and the right to petition the government for a redress of grievances. The Fourth Amendment protects the people from unreasonable searches and seizures and requires that warrants be issued only upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the individual or things to be seized. The Sixth Amendment establishes the right of an accused individual to a speedy and public trial by an impartial jury, to be informed of the nature and cause of the charges, to confront witnesses, to have compulsory process to obtain witnesses, and to have the assistance of legal counsel. The Fourteenth Amendment addresses citizenship rights and equal protection of the laws. Although the equal protection clause applies explicitly only to state governments, equal protection requirements apply to the federal government through the Fifth Amendment Due Process Clause.

14. **Section 210401 of the Violent Crime Control and Law Enforcement Act of 1994, 42 U.S.C. § 14141—** This is a federal statute that provides that it shall be unlawful for any governmental authority or its agent to engage in a pattern or practice of conduct by law enforcement officers that violates the Constitution or laws of the United States. It authorizes the Attorney General to bring civil actions to obtain injunctive or declaratory relief to eliminate the unlawful or unconstitutional pattern or practice.

Appendix D—Cases and Authorities

A. Fourth Amendment Privacy Law

Katz v. United States, 389 U.S. 347 (1967), provides the foundation for most federal court privacy rulings and doctrines. *Katz* moved away from previous Supreme Court privacy jurisprudence in holding that the Fourth Amendment protects people and not places and departed from the previous "trespass" doctrine of Fourth Amendment protection. Fourth Amendment considerations no longer required a physical invasion or trespass. This case began with federal charges placed against defendant Charles Katz for violating a federal law prohibiting the use of interstate communications for placing wagers and bets. Law enforcement had witnessed Katz making calls from a public telephone booth and thereafter placed microphones on the exterior of the telephone booth in order to eavesdrop on his private conversations. The Court found that no physical invasion of the phone booth had occurred but stated that this was not necessary to constitute a search for purposes of the Fourth Amendment. Rather, *Katz* established a two-prong test to determine whether the Fourth Amendment is implicated and a search has occurred. If an individual, like Katz, has manifested an intent to make the information private *and* society accepts that expectation of privacy as reasonable, then that privacy expectation cannot be violated without following Fourth Amendment warrant requirements. In this case, the Court stated that the defendant assumed his conversations were private because he sought to exclude others when he entered the enclosed telephone booth. The Court concluded, "The government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied when using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."

Smith v. Maryland, 442 U.S. 735 (1979), forms the basis of the "third-party exposure" doctrine of electronic privacy law. In Smith, the government used pen register technology to record the numbers dialed out from a certain phone number. This information was used to convict the defendant of robbery. The defendant challenged the use of the pen register as an illegal search under the Fourth Amendment. The *Smith* Court explained that "[c]onsistently with *Katz*, this Court uniformly has held that the application of the Fourth Amendment depends on whether the individual invoking its protection can claim a 'justifiable,' a 'reason,' or a 'legitimate expectation of privacy' that has been invaded by government action. This inquiry . . . normally embraces two discrete questions. The first is whether the individual, by his conduct, has exhibited an actual (subjective) expectation of privacy' . . . . The second question is whether the individual's subjective expectation of privacy is 'one that society is prepared to recognize as reasonable.'" Id. at 740. The Court held that the defendant did not have a reasonable expectation of privacy in the phone record information because the information was automatically turned over to a third party, the phone company. Even if the defendant had an expectation of privacy in the numbers dialed, it was not one society recognized as reasonable—therefore, there was no Fourth Amendment violation.

United States v. Knotts, 460 U.S. 276, 280 (1983) (citing *Katz v. United States*, 389 U.S. 347 (1967)), examined whether a defendant had a reasonable expectation of privacy when travelling on public streets and highways. In *Knotts*, law enforcement placed a beeper in a drum of chloroform in order to track the movements of the vehicle holding the container. The information derived from the radio beeper led the police to a remote cabin where a warrantless search revealed a drug lab. The Court relied heavily on a quote from ***Smith v. Maryland***, 442 U.S. 735 (1979), elaborating on the principles articulated in *Katz*. See *Knotts*, 460 U.S. at 480-081, quoting *Smith*, 442 U.S. at 740. ("Consistently with

Katz, this Court uniformly has held that the application of the Fourth Amendment depends on whether the individual invoking its protection can claim a 'justifiable,' a 'reason,' or a 'legitimate expectation of privacy' that has been invaded by government action. This inquiry . . . normally embraces two discrete questions. The first is whether the individual, by his conduct, has exhibited an actual (subjective) expectation of privacy' . . . . The second question is whether the individual's subjective expectation of privacy is 'one that society is prepared to recognize as reasonable.'") Applying this test, *Knotts* determined that tracking the vehicle did not constitute a search because an "individual travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another" and noted that such movements could have been observed by the naked eye.

United States v. Karo, 468 U.S. 705, 708 (1984), is a case in which a U.S. Drug Enforcement Administration (DEA) agent learned that defendants had ordered 50 gallons of ether from a government informant, who explained that the ether was to be used to extract cocaine from clothing that had been imported into the United States. The government obtained a court order authorizing the installation and monitoring of a beeper in a can of ether, which allowed the government to track the defendant's location. The ether was moved in succession to multiple locations. The information from the beeper led the government to a private residence. Using information derived from the beeper, the government obtained and executed a search warrant, which led to the discovery and seizure of cocaine. Relying on *Katz* and *Knotts*, the Court held that locational information received while the radio transmitter was on public roads was constitutional because Defendant Karo did not have a reasonable expectation of privacy while driving on the roads. However, monitoring the beeper while it was in a private residence, a location that is not opened to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of that residence. On this latter holding, the *Karo* Court distinguished *Knotts* on the grounds that the beeper was not monitored while it was located in a private residence.

Kyllo v. United States, 533 U.S. 27 (2001), establishes the Supreme Court rule on advanced technology use in searches. In *Kyllo*, the police suspected the defendant of growing marijuana inside his residence. They utilized thermal imaging equipment to "peer through" the walls of the home and determined the defendant was growing marijuana. The court of appeals upheld the search on the basis that the defendant did not make any effort to conceal the heat emanating from his home and therefore did not have a reasonable expectation of privacy under the Fourth Amendment. The Supreme Court reversed, holding that the thermal imaging infiltrated the home and did constitute a search under the Fourth Amendment. The Supreme Court ruled that it was a search in violation of the Fourth Amendment because the thermal imaging gained information, through technology not generally used by the public that could not have otherwise been gained without physical intrusion of the home, a constitutionally protected area without a warrant.

United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), is a case that addressed the constitutionality of the warrantless use of a GPS device by examining the privacy risks associated with prolonged collection of location information. The *Maynard* Court stated that those employing GPS trackers "can deduce whether the individual being tracked is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about an individual, but all such facts." Id. at 562. Under this theory, discrete bits of data, when compiled and viewed together over time, may create a mosaic of the individual's habits, relationships, and beliefs. The Court thus extended the privacy protections articulated in *Katz* to situations in which extensive tracking of public movements would reveal a composite profile, when compiled, about an individual and thus held that the police action was a search because it defeated the defendant's reasonable expectation of privacy. Accord *United States v. Jones,* 132 S. Ct. *945, 954 (2012)* (Sotomayor, concurring); but see Orin S. Kerr, The Mosaic Theory of the Fourth Amendment, 111 MICH L. REV. 311 (2012)).

United States v. Jones, 132 S. Ct. 945 (2012), is a case involving law enforcement's placement of a Global Positioning System (GPS) device on a subject's car and use of the device to monitor the vehicle's movement on public streets for a four-week period (which extended beyond the period of time and place authorized by a search warrant). Citing *Katz*, the government argued that no search occurred because Jones had no reasonable expectation of privacy in the area of the vehicle accessed by the government and in the locations of the vehicle on the public roads since they were visible to the public. The Supreme Court Justices rejected this argument and unanimously agreed that use of the GPS device constituted a search within the meaning of the Fourth Amendment. The majority explained that a physical intrusion into a constitutionally protected area, coupled with an attempt to obtain information, can constitute a violation of the Fourth Amendment based upon a theory of common law trespass. The majority explained that "the use of longer-term GPS monitoring in investigations of most offenses impinges on expectations of privacy." Additionally, in a separate opinion, Justice Sotomayor explained that it may be time to rethink all police use of tracking technology, not just long-term GPS, reasoning that "GPS monitoring generates a precise, comprehensive record of an individual's public movement that reflects a wealth of detail about her familial, political, religious, and sexual associations . . . .The government can store such records and efficiently mine them for years to come."

The unanimous decision in ***Riley v. California***, 134 S. Ct. 2473 (2014), demonstrated the United States Supreme Court's willingness to extend Fourth Amendment protections to mitigate the privacy risks associated with the use of new technologies. The Court contrasted a search of information on the cell phone with a search of physical items, saying that such analogy is akin to "saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from Point A to Point B but little else justified lumping them together." The Court also emphasized that "the fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone-seized incident to an arrest is accordingly simple—get a warrant."

B. ALPR and Privacy Law

New Jersey v. Donis, 157 N.J. 44 (N.J. 1998). The New Jersey Supreme Court has held that police are permitted to randomly (i.e., without probable cause) check a license plate number against the state DMV database of any vehicle they encounter while on patrol, accessing only public information such as registration, license status, and whether the car has been reported as stolen. If the inquiry discloses a basis for further police action, then the officer may access the personal information of the registered owner. This case establishes a nondisclosure rule to protect the legitimate privacy interests of motorists.

United States of America v. Curtis Ellison, 462 F.3d 557 (6th Cir. 2006), *cert. denied*, 552 U.S. 947 (2007). The United States Court of Appeals for the Sixth Circuit held that random license plate checks are not an unconstitutional invasion of privacy and that "so long as the officer had a right to be in a position to observe the defendant's license plate, any such observation and corresponding use of the information on that plate does not violate the Fourth Amendment." In reaching this holding, the *Ellison* Court relied on a central tenet of Fourth Amendment jurisprudence established in ***Katz v. United States***, 389 U.S. 347 (1967)—"that the Fourth Amendment protects only what an individual seeks to keep private," and recognized that "objects falling in the plain view of an officer who has a right to be in the position to have that view are subject to seizure . . . ." Id. at 561 (*internal citation omitted*). The court analogized license plates to an automobile's Vehicle Identification Number (VIN), "located inside the passenger compartment, but visible from outside the car," and noted that a VIN does not receive Fourth Amendment protection. Like a VIN, the purpose of a license plate number is "to provide identifying information to law enforcement officials and others." Quoting and applying the reasoning in ***New York v. Class***, 475 U.S. 106 (1986), regarding VINs, the *Ellison* Court determined that "because of the important role played by the [license plate] in the pervasive governmental regulation of the automobile and the efforts by the Federal Government to ensure that the [license plate] is placed in plain view," a motorist can have no reasonable expectation of privacy in the information contained on it. ***Ellison***, 462 F.3d at 561, quoting ***Class***, 475 U.S. at 114.

The ***Ellison*** Court also rejected the notion that the entry of the license plate number into a law enforcement database creates a privacy interest in the nonprivate information retrieved in response to a query, reasoning that "[t]he obvious purpose of maintaining law enforcement databases is to make information, such as the existence of outstanding warrants, readily available to officers carrying out legitimate law enforcement duties." In fact, the computer investigation in this case was "far less invasive than other government actions that fall" outside the purview of the Fourth Amendment. ***Ellison***, 462 F.3d at 562, citing ***Oliver v. United States,*** 466 U.S. 170, 177, 104 S.Ct. 1735, 80 L.Ed.2d 214 (1984) (entering private property with "No Trespassing" signs to observe marijuana plants in an "open field" not visible from outside the property); ***Dow Chemical Co. v. United States,*** 476 U.S. 227, 239, 106 S.Ct. 1819, 90 L.Ed.2d 226 (1986) (photographing an industrial complex with a precision aerial mapping camera); ***California v. Ciraolo,*** 476 U.S. 207, 213-14, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986) (using aerial surveillance in public airspace to observe the curtilage of a private residence); and ***Smith v. Maryland,*** 442 U.S. 735, 745-46, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979) (placing a pen register on a phone line to record the numbers dialed from a private residence). This case is distinguishable from a situation in which the police use a technology not available to the public to discover evidence that could not otherwise be obtained without "intrusion into a constitutionally-protected area." ***Kyllo v. United States,*** 533 U.S. 27, 34-35, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) (holding that the use of thermal-imaging technology to detect heat inside a private home violates the Fourth Amendment). The ALPR technology used in this case does not enable law enforcement to access any previously unobtainable information; it simply allows them to access information more quickly. Given that the information was obtained without intruding upon a constitutionally protected area, the *Ellison* Court held that there was no "search" for purposes of the Fourth Amendment. ***Ellison***, 462 F.3d at 563, citing ***United States v. Matthews,*** 615 F.2d 1279, 1285 (10th Cir. 1980); ***United States v. Walraven,*** 892 F.2d 972, 974 (10th Cir.1989); ***Olabisiomotosho v. City of Houston,*** 185 F.3d 521, 529 (5th Cir.1999); ***United States v. Sparks,*** 37 Fed. Appx. 826, 829 (8th Cir.2002); ***Hallstein v. City of Hermosa Beach,*** 87 Fed.Appx. 17, 19 (9th Cir.2003); ***United States v. $14,000.00 in U.S. Currency,*** No. 98-4380, 2000 WL 222587, at *3 (6th Cir. Feb. 14, 2000) (finding no Fourth Amendment violation in a computer check of a license plate); ***United States v. Batten,*** 73 Fed. Appx. 831, 832 (6th Cir. 2003; *see also* **WAYNE R. LAFAVE**, 1 Search & Seizure § 2.5(b) (4th ed. 2004).

The decision in ***Ellison*** has been extensively cited for the proposition that a "motorist has no reasonable expectation of privacy in information contained on his license plate under the Fourth Amendment." See, e.g., ***Yamba v. Harper***, 2010 U.S. Dist. LEXIS 21288 (W.D. Pa. Mar. 9, 2010); ***Cincerella v. Egg Harbor Twp. Police Dep't***, 2009 U.S. Dist. LEXIS 22950 (D.N.J. Mar. 23, 2009); ***United States v. Crooks***, 2008 U.S. Dist. LEXIS 35189 (D. Del. Apr. 29, 2008); ***United States v. Lurry***, 2010 U.S. Dist. LEXIS 118494 (W.D. Tenn. Nov. 8, 2010); ***Brooks. v. Pickett***, 2008 U.S. Dist. LEXIS 27796 (E.D. Mich. Apr. 7, 2008); ***United States v. Miranda-Sotolongo***, 2016 U.S. App. LEXIS 11816 (7th Cir. Ill. June 28, 2016); ***United States v. Diaz-Castaneda***, 494 F.3d 1146, 2007 U.S. App. LEXIS 17005 (9th Cir. Or. 2007); ***Martinez v. State***, 2010 Del. Super. LEXIS 195 (Del. Super. Ct. Apr. 29, 2010); ***Milam v. Commonwealth***, 2013 Ky. App. Unpub. LEXIS 992 (Ky. Ct. App. Aug. 30, 2013); ***Gentry v. Commonwealth***, 2012 Ky. App. Unpub. LEXIS 1040 (Ky. Ct. App. Oct. 12, 2012); ***State v. Sloan***, 193 N.J. 423, 939 A.2d 796, 2008 N.J. LEXIS 22 (2008).

C. Implications of Automation

U.S. Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989). The U.S. Supreme Court acknowledged the distinction between public records that might result from a diligent search of courthouse files, county clerks' offices, and local police stations throughout the United States and a computerized summary maintained in a single clearinghouse of information. The Court held that the electronic compilation of otherwise publicly available but hard to obtain information changed the privacy interest implicated by disclosure of that compilation. The process of automation overcame the "practical obscurity" associated with manually collecting and linking the public records associated with a particular individual into a comprehensive criminal history record. (Note: The Society of American Archivists defines *practical obscurity* as "the principle that private information in public records is effectively protected from disclosure as a result of practical barriers to access." *Practical Obscurity*, SOC'Y AM. ARCHIVISTS, available at http://www2.archivists.org/glossary/terms/p/practical-obscurity.)

D. Civil Rights and Civil Liberties

Green v. City & County of San Francisco, 751 F.3d 1039 (9th Cir. 2014), arose out of a vehicular stop performed by an officer after the agency's automatic license plate reader mistakenly identified the car that a woman was driving as a stolen vehicle. She was stopped, held at gunpoint by multiple officers, handcuffed, forced to her knees, and detained for up to 20 minutes and released once the officers ran her plate and discovered the ALPR mistake and that her vehicle was not stolen. The Ninth Circuit Court of Appeals reversed the district court's grant of summary judgment in favor of the defendant, reinstating the plaintiff's claims of a Fourth Amendment violation and instructing that such claims raised questions of fact for a jury. See also **Department of Homeland Security, *Privacy Impact Assessment for the Acquisition and Use of LPR Information from a Commercial Service,*** at 7 (2013), citing ***Green***, 751 F.3d 1039, and identifying misidentification of a vehicle and its occupants as a privacy risk. ("A license plate read sent to ICE may be incomplete or inaccurate because the license plate is bent, dirty, or damaged, or because the individual reading the numbers makes an error. This can result in the misidentification of a vehicle and its occupants.")

$14,000 in U.S. Currency, 211 F.3d 1270, 2000 U.S. App. Lexis 2429 (6th Cir. 2000). The claimant filed a motion to suppress the $14,000 subject to the forfeiture proceedings, arguing constitutional violations. With regard to the claimant's Fourteenth Amendment claim, the court acknowledged that "it would violate the Equal Protection Clause of the Fourteenth Amendment for an officer to run computer checks in an 'intentionally racially discriminatory manner," citing ***United States v. Travis,*** 62 F.3d 170, 174 (6th Cir. 1995), cert. denied in 516 U.S. 1060, 116 S. Ct. 738 (1996) ("consensual searches may violate the Equal Protection Clause when they are initiated solely based on racial considerations"). The claimant's Equal Protection claim was rejected by the court because the claimant failed to meet his burden of proof of establishing that the officer decided to conduct the computer check of his license plate based solely upon the race of the claimant and the other occupant in the car.

E. Guidance and Policy

International Association of the Chiefs of Police, *Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement*, at 32 (2012), advising that agencies using ALPR technology should address a range of privacy issues, including "[w]hat ALPR information is collected, how the information is collected, how long the information are retained, who can access the information and for what purposes, and what kind of analytic tools and methodologies are available to query and use ALPR information."

U.S. Department of Homeland Security, *Privacy Impact Assessment for the Acquisition and Use of LPR Information from a Commercial Service,* at 7 (2013), available at https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-lpr-march2015.pdf. As explained in this PIA, U.S. Immigration and Customs Enforcement (ICE) uses information obtained from LPRs as one investigatory tool in support of its criminal investigations and civil immigration enforcement actions (i.e., in furtherance of open cases, investigations, or ongoing enforcement actions and only when

necessary based on a law enforcement need). This PIA assesses the potential impact of the use of information obtained from LPRs on the civil liberties of the public and explains the measures to be put in place, in addition to the framework of privacy and civil liberties protections, to mitigate such concerns.

U.S. Department of Justice, *Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity* (December 2014), at https://www.justice.gov/sites/default/files/ag/pages/attachments/2014/12/08/use-of-race-policy.pdf, articulating the standards that should guide use by federal law enforcement officers of race, ethnicity, gender, national origin, religion, sexual orientation, and gender identity in law enforcement or intelligence activities.

(This Page Intentionally Left Blank)

Appendix E—Sample LPR Policy

The following is a sample LPR Policy that contains all of the sample policy language shown after each question in the template section of this document. However, while drafting an LPR policy using this language, it is important that the policy author still review each question and its associated guidance in the template section in tandem with customizing this language. To assist with this task, the policy language contained here mirrors the same structure and policy categories as those reflected in the template so that the template questions may be followed, item by item, while customizing this language. Further, it is critical that entities drafting a policy not cut and paste this language and use it as is, without making modifications. There are many areas that prompt for insertions and entity customization. These are shown **bolded and in brackets [ ]**. Also, this policy may not cover all concepts that are unique to your entity's specific LPR program or there may be provisions that are not applicable that should be deleted. Throughout the sample policy, law enforcement entities are encouraged to enhance language with references to applicable statutes, rules, standards, or policies.

Finally, since this guidance resource promotes transparency with the public, entities should ensure their policy is written not only for the understandability of entity personnel but also for the understandability of members of the public. While some of the provisions here may reflect concepts and processes long understood and integrated into the daily work of law enforcement such that an entity may not feel they are necessary in the policy, they are still provided here for the purposes of informing the general public, who may not be aware of such processes, and articulating the entity's position and procedures for protecting privacy, civil rights, and civil liberties throughout the entity LPR program.

A. Purpose Statement

1. It is the purpose of this policy to provide **[name of entity]** personnel with guidelines and principles for the collection, access, use, dissemination, retention, and purging of LPR information to ensure that the information is used for legitimate law enforcement purposes only and that privacy, civil rights, and civil liberties of individuals are not violated. The Fair Information Practice Principles (FIPPs) form the core of the privacy framework for this policy.

This policy assists **[name of entity]** and its personnel in:

- Increasing public safety and improving state, local, tribal, territorial, and national security.
- Minimizing the threat and risk of injury to specific individuals.
- Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.
- Promoting governmental legitimacy and accountability.
- Minimizing the potential risks to individual privacy, civil rights, civil liberties and other legally protected interests.
- Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information.
- Minimizing the threat and risk of damage to real or personal property.
- Increasing trust by maximizing transparency.
- Making the most effective use of public resources allocated to public safety entities.

2. The provisions of this policy are provided to support authorized uses of LPR information. Authorized uses may include the following **[include any of the following purposes or others that apply to the entity]**:

- Enhance **[insert state]**'s AMBER/SILVER or other law enforcement alerts and real-time response capability by deploying and networking LPRs across the state to more rapidly identify and locate vehicles related to potential child-abduction or other serious crimes.
- Alert law enforcement that a particular license plate on a "hot list" (e.g., a stolen vehicle or a vehicle associated with a wanted individual) is in close proximity to an LPR to dramatically reduce the recovery time of stolen vehicles and assist in locating dangerous and wanted individuals.
- Identify plates associated with potential witnesses and/or victims of violent crime.
- Support **[name of entity]**'s homeland security mission by protecting critical infrastructure from individuals who intend to damage or disrupt the systems and locations that allow for travel and the free flow of commerce.
- Identify vehicles linked to stolen license plates or other motor vehicle traffic violations.
- Provide situational awareness for law enforcement related to public safety or otherwise relevant to their authorized duties.
- Support local, state, federal, and tribal public safety departments in the identification of subjects associated with/as targets of criminal investigations.
- Support law enforcement response to critical incident responses and special events.
- Support special operations, such as high-crime-area patrols, gang investigation/suppression, driving under the influence initiatives, enforcement details, directed criminal investigations, and other investigations.

B. Policy Applicability and Legal Compliance

1. This policy applies to LPR information collected or received, accessed, used, disseminated, retained, and purged by the **[name of entity]**. It is not intended to apply and does not apply to any other types of information accessed, retained, or used by the **[name of entity]**.

2. All **[name of entity]** personnel, participating agency personnel and authorized individuals working in direct support of **[name of entity]** personnel (such as interns), personnel providing information technology services to the **[name of entity]**, private contractors, and other authorized users will comply with the **[name of entity]**'s LPR policy. This policy applies to information the **[name of entity]** collects or receives, accesses, uses, disseminates, retains, and purges.

3. The **[name of entity]** will provide a printed or electronic copy of this LPR policy to all:

- **[name of entity]** and non-**[name of entity]** personnel who provide services.
- Participating agencies.
- Individual authorized users.

The **[name of entity]** will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the applicable provisions it contains.

4. All **[name of entity]** personnel, participating agency personnel and authorized individuals working in direct support of **[name of entity]** personnel (such as interns), personnel providing information technology services to the **[name of entity]**, private contractors, agencies from which **[name of entity]** information originates, and other authorized users will comply with applicable laws and policies concerning privacy, civil rights, and civil liberties, including, but not limited to **[include a specific reference to any relevant state statutes or other binding state or local policy specific to LPR systems, then provide a list of other applicable state and federal privacy, civil rights, and civil liberties laws or include a reference to the section or appendix containing a list of applicable law]**. As part of this process, all individuals working with LPR information will complete the applicable training as directed by **[name of entity]**.

C. Governance and Oversight

1. Primary responsibility for the operation of the **[name of entity]**; its justice information systems, operations, and the coordination of personnel; the receiving, seeking, retention, evaluation, information quality, use, purging, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the **[position/title]** of the **[name of entity]**.

2. The **[name of entity]**'s **[insert title]** will designate an LPR Administrator who will be responsible for the following **[include any of the following responsibilities that apply to the LPR Administrator or other responsibilities]**:

- Overseeing and administering the LPR program.
- Ensuring that stored LPR information is automatically purged from the LPR database, unless determined to be of evidentiary value (refer to Section K.1, Information Retention and Purging).

- Confirming, through random audits, that LPR information is purged in accordance with this policy.
- Acting as the authorizing official for individual access to the LPR information.
- Ensuring and documenting that all personnel with authorized access to LPR information are trained prior to using the system.
- Conducting audits to ensure compliance with applicable laws, regulations, standards, and policy.

3. The **[name of entity]** is guided by a **[insert guiding authority, for example, a "designated LPR oversight committee"]** that liaises with the community to ensure that privacy, civil rights, and civil liberties are appropriately protected by this LPR policy and by the **[name of entity]**'s LPR information collection, receipt, access, use, dissemination, retention, and purging processes and procedures.

Approach 1: The committee will annually review and update the LPR policy in response to changes in law and implementation experience, including the results of audits and inspections and will solicit input from stakeholders on the development or proposed updates to the LPR policy.

Approach 2: The committee will annually review and update the LPR policy in response to changes in law and implementation experience, including the results of audits and inspections and provide notice to and solicit comment from the public on the development or proposed updates to the LPR policy.

4. The **[insert title of individual or name of entity]** will receive reports regarding alleged errors and violations of the provisions of this LPR policy, will receive and coordinate complaint resolution under the **[name of entity]**'s LPR redress policy, and will ensure that privacy, civil rights, and civil liberties protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The **[insert title of individual but not the name or name of entity]** may be contacted at the following address: **[insert mailing address or e-mail address]**.

5. The **[name of entity]**'s **[insert title]** will ensure that enforcement procedures and sanctions outlined in **[insert section number of policy (see Section L.3, Enforcement)]** are adequate and enforced.

D. Definitions

1. For examples of primary terms and definitions used in this LPR policy, refer to **[insert section or appendix citation]**.

E. Acquiring and Receiving LPR Information

1. The **[name of entity]**, through its **[insert name of the entity's LPR program]**, will directly collect and retain LPR information that:

- Is based on a potential threat to public safety or the enforcement of the criminal law, or
- Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity, or
- Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences, or
- Is directly related to an investigation or mission of the law enforcement entity, and
  - The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
  - The information was collected in a fair and lawful manner (e.g., it does not infringe on the federal or state constitutional rights of any individual, group, or organization).

The **[name of entity]** will indirectly acquire LPR information from **[list other law enforcement agency or agencies]** in accordance with **[insert mechanisms, e.g., MOU, law, intergovernmental or interagency agreement]** established between the **[name of entity]** and the law enforcement agency(ies).

2. The **[name of entity]** will query **[insert name of law enforcement or commercial database]** LPR information that:

- Is based on a possible threat to public safety or the enforcement of the criminal law, or
- Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any

individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity, or
- Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime, or
- Is directly related to an investigation or mission of the law enforcement entity, and
  - The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
  - The information was collected in a fair and lawful manner.

3. Hot-list information is considered confidential information to the extent permitted by law and will be updated **[insert time period(s)]** each day. Officers assigned an LPR unit are responsible for ensuring they are operating with the most current hot list (at minimum) at the beginning of each shift, including information files of stolen and "of interest" vehicles containing all of the current National Crime Information Center (NCIC) information. Department members will query their LPR system to ascertain whether there is a prior read of the license plate that is the subject of the particular alert, bulletin, or alarm. Proactive manual entry of LPR hot lists in the field is permitted for:

- Dispatched reports of crimes—"Be On the Lookouts" (BOLOs) or AMBER, SILVER, or other law enforcement alerts in which a license plate number is part of the broadcast; or
- When directed or authorized for a legitimate law enforcement purpose.

4. The **[name of entity]** and any information-originating entities will not seek, submit, or retain LPR information about individuals or organizations based solely on their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, gender identity, sexual orientation, or other classification protected by law.

5. **[Name of entity]** LPR cameras may be mobile (mounted on vehicles) or stationary (mounted to a structure). A standard LPR record contains, at a minimum, an optical character recognition (OCR) interpretation of the captured image, a photo of the license plate and a contextual photo of an area surrounding the plate that could range from a few inches to a larger area around the entire vehicle, the geographic coordinates of where the image was captured, the date and time of the recording, and the specific camera/unit that captured the image.

6. **[Name of entity]**-accessed LPR information contains images of license plates that are available to public view (e.g., vehicles that are on a public road or street or that are on private property but whose license plates[s] are visible from a public road, street, or place to which members of the public have access, such as the parking lot of a shop or other business establishment) and that identify specific vehicles. Retained LPR information does not include specific identification of individuals. Separate video surveillance images of the same location or images from private cameras will not be associated with LPR data unless a specific image is required to investigate or document a violation in accordance with the authorized purposes described in this section.

License plate numbers and date/time location collected through an LPR may not be, when taken alone, sufficient to identify the individual associated with the vehicle. The **[name of entity]** may be able to link the LPR information to an individual through additional use and combination with other information, such as a check of vehicle registration. Thus, even though the LPR information the **[name of entity]** accesses may be the result of an LPR system's automated collection of license plate numbers, it is the investigation process that identifies individuals. Refer to Section H.2 for information on the **[name of entity]**'s LPR validation procedure or to Appendix A, Glossary of Terms and Definitions, for more information on LPR information.

Approach 1:
The **[name of entity]** protects all LPR information as personally identifiable information (PII) because LPR information may be combined with other information to specify a unique individual (i.e., the identity of an individual could be directly or indirectly inferred by using information that is linked or linkable to that individual). The **[name of entity]** collects, receives, accesses, uses, disseminates, retains, and purges LPR information because it can be linked to an individual to further an authorized mission. **[For those entities that withhold LPR information from public release using the privacy exemption under public records laws, Approach 1 should be selected.]**

Approach 2:
In the absence of the investigation process, the license plate number and the time and location data attached to it may not identify a specific person. Thus, even though the **[name of entity]**'s LPR systems automate the collection of license plate numbers, it is the investigation process that identifies individuals. Refer to Section H.2 for information on the **[name of entity]**'s LPR validation procedure or to Appendix A, Glossary of Terms and Definitions, for more information on LPR information.

Databases of LPR information do not contain alert lists based on strictly civil matters. In addition, LPR information does not contain audio recordings.

7. Per the **[name of entity]** policy of nondiscrimination noted in Section E.4, the pattern and frequency of stationary camera placement will be assessed **[note frequency]** to confirm nondiscriminatory placement.

8. The hardware and software licenses associated with the **[name of entity]**'s LPR system are the property of **[insert name of owning agency]**, regardless of whether the system has been purchased, leased, or acquired as a service. All deployments of the LPR system are for official use only (FOUO). All information captured, stored, generated, or otherwise produced by an LPR system is the property of the **[insert name of owning agency]**, regardless of where the information is housed or stored.[1]

9. LPR information collection and investigative techniques used by the **[name of entity]** and by LPR information-originating agencies must be the least intrusive as necessary in the particular circumstances to collect LPR information the **[name of entity]** is authorized to seek or retain.

10. The **[name of entity]** will contract only with commercial LPR database companies that provide an assurance that their methods for collecting, receiving, accessing, disseminating, retaining, and purging LPR information comply with applicable local, state, tribal, territorial, and federal laws, statutes, regulations, and policies and that these methods are not based on misleading information collection practices.

11. The **[name of entity]** will not directly or indirectly seek, receive, accept, or retain LPR information from:

    - An individual who or nongovernmental agency that may receive a fee or benefit for providing the LPR information, except as expressly authorized by law or **[name of entity]** policy, and/or
    - An individual who or information provider that is legally prohibited from obtaining or disclosing the LPR information.

F. Use of LPR Information

1. Access to or disclosure of LPR information will be provided only to individuals within the **[name of entity]** or in other governmental agencies who are authorized to have access and only for legitimate law enforcement purposes (e.g., enforcement, reactive investigations) and to IT personnel charged with the responsibility for system administration and maintenance. This means that queries and dissemination of LPR information are permitted only if:

    - There is a legal basis requiring these actions, or
    - There is reasonable suspicion that an individual or enterprise is involved in criminal conduct or activity, and
        - The LPR information is relevant to that suspected criminal conduct or activity and the requestor has a legitimate need to know.

    Authorized uses are described in A.2 of this policy. However, the **[name of entity]** accords special consideration to the collection of LPR information relating to First Amendment-protected events and will articulate a legal or justified basis for such collection during the planning assessment and approval process for the particular event, before proceeding with the collection.[2]

2. The **[name of entity]** will prohibit access, use, or dissemination of LPR information for:

    - Any purpose that violates the Constitution or laws of the United States, including the protections of the Fourth Amendment.
    - Non-law enforcement or personal purposes.
    - Discriminatory purposes.
    - The purpose of prohibiting, infringing upon, or deterring individual activities protected by the First Amendment, such as freely practicing one's religion, freedom of speech and peaceful assembly, freedom of the press, and the right to petition the government for the redress of grievances.[3]
    - The purpose of prohibiting or deterring lawful individual exercise of other rights, such as freedom of association, implied by and secured by the U.S. Constitution or any other constitutionally protected right or attribute.
    - Harassing and/or intimidating any individual or group.
    - Targeting of any individual or group by means of camera placement or data use in a discriminatory manner, noted in Section E.4.
    - Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

3. In addition, the **[name of entity]** will employ credentialed, role-based access criteria, as appropriate, to control:

   - The LPR information to which a particular group or class of users may have access based on the group or class.
   - The assignment of roles (e.g., administrator, manager, operator, and user).
   - The categories of LPR information that a class of users are permitted to use in order to update a hot list, including information being utilized in specific investigations.
   - Any administrative or functional access required to maintain, control, administer, audit, or otherwise manage the information or equipment.

G. Sharing and Dissemination of LPR Information

1. The **[name of entity]** will establish requirements for any external agency requesting access to the **[name of entity]**'s LPR information. These requirements will be documented in an interagency agreement/memorandum of understanding and will include an assurance from the external agency that it complies with the laws and rules governing those individual agencies, including applicable federal and state laws.

2. The **[name of entity]**'s LPR information **will not** be:

   - Sold, published, exchanged, or disclosed to commercial or private entities or individuals except as required by applicable law and to the extent authorized by the **[name of entity]**'s agreement with a commercial vendor.
   - Disclosed or published without prior notice to the originating entity that such information is subject to disclosure or publication. However, the **[name of entity]** and the originating agency may agree in writing in advance that the **[name of entity]** will disclose LPR information as part of its normal operations, including disclosure to an external auditor of the LPR information.
   - Disclosed on a discretionary basis unless the originating agency has provided prior written approval or unless such disclosure is otherwise authorized by the memorandum of understanding or agreement between the **[name of entity]** and the originating agency.
   - Disclosed to unauthorized individuals.

3. The **[name of entity]** will not confirm the existence or nonexistence of LPR information to any individual or agency that would not be authorized to receive the information unless otherwise required by law.

H. Information Quality Assurance

1. Original LPR information will not be altered, changed, or modified in order to protect the integrity of the data. Any changes will be maintained as a separate and additional record, and such record will be identified as having been modified.

2. Whenever a license plate reader alerts on license plate information, prior to taking any law enforcement action, officers will be required, to the fullest extent possible, to visually verify that the actual vehicle license plate information matches the license plate information used and alerted upon by the LPR system, including both alphanumeric characters of the license plate and the state of issuance; verify the current status of the plate as active through **[insert name of source, such as mobile information terminal [MDT] query, NCIC, etc.]**; and confirm whether the alert pertains to the registrant of the car or the car itself. Receipt of an LPR alert for a stolen or felony vehicle may not rise to the level of reasonable suspicion and is not sufficient probable cause to arrest without confirmation that the alert is still valid and active. If the alert is for another type of transaction, the officer will read the description of the alert and follow the appropriate action or reporting method. If an LPR alert cannot be verified both visually and for validity, then law enforcement should not act on the alert and it should be rejected.

   If the officer witnesses a violation of law or other action that establishes reasonable suspicion for a stop, the officer may conduct a stop based on that reasonable suspicion. This provision shall not prevent a law enforcement officer from taking immediate action when a verifiable emergency situation exists for officer safety.

   On each resulting alert, the officer is required to enter a disposition indicating the action taken or not taken on the alert.

3. The **[name of entity]** will perform routine maintenance, upgrades, calibration, and refreshes of all LPR equipment and components to ensure proper functionality, including the following:

   - At the beginning of a shift, officers will visually inspect the exterior cameras to ensure the lenses are clear and the cameras have not been altered in any way.

- Designated, trained personnel shall check LPR equipment on a regular basis to ensure functionality and proper camera alignment.
- Any equipment that falls outside expected functionality shall be removed from service until deficiencies have been corrected.
- Officers will not attempt to disconnect, modify, or change the LPR equipment or software unless authorized to do so.
- Damage or other malfunctions to the equipment will be reported to the **[insert position/title]**.
- The LPR equipment and components will not be transferred to another vehicle except with the prior, written approval of the LPR Administrator.

4. The **[name of entity]** will investigate, in a timely manner, alleged errors and deficiencies of LPR information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and deficiencies.

5. The **[name of entity]** will correct, notate, delete, or refrain from using LPR information the **[name of entity]** originated and found to be erroneous or deficient. Originating agencies external to the **[name of entity]** are responsible for reviewing the quality and accuracy of the LPR information provided to the **[name of entity]** and must take reasonable steps to correct or amend the information upon learning that it is inaccurate or deficient. The **[name of entity]** will review the quality of LPR information it has received from an originating agency or vendor and will advise the appropriate point of contact, in writing or electronically, when its LPR information is alleged, suspected, or found to be erroneous or deficient.

6. The **[name of entity]** will use written or electronic notification to inform recipient agencies **[or, if applicable, use the phrase "inform the consolidated system"]** when LPR information previously provided is erroneous or deficient. In addition, the **[name of entity]** will take reasonable steps to correct or amend the information provided to the external agency in order to ensure accuracy and sufficiency to the extent possible.

I. Redress

I. 1 Disclosure

1. LPR information will be disclosed to the public in accordance with **[cite applicable public records laws]**. **[If your state law permits disclosure, revise provision to reflect this.]**

2. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity, an individual is entitled to know the existence of and to review the LPR information about him or her that has been collected or received and retained by the **[name of entity]**. If allowed by state law, the individual may obtain a copy of the LPR information for the purpose of challenging the accuracy or completeness of the information (correction). The **[name of entity]**'s response to the request for LPR information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests.

I. 2 Corrections

1. If, in accordance with state law, an individual requests correction of LPR information *originating with the* **[name of entity]** that has been disclosed, the **[name of entity]**'s **[insert title of designee]** will inform the individual of the procedure for requesting corrections, including appeal rights for those requests that are denied in whole or in part. A record will be kept of all requests.

I. 3 Appeals

1. The individual who has requested disclosure or to whom LPR information has been disclosed will be informed of the reason(s) why the **[name of entity]** or originating agency denied the request for disclosure or correction. The individual will also be informed of the procedure for appeal when the **[name of entity]** or originating agency has cited an exemption for the type of information requested or has declined to correct challenged LPR information to the satisfaction of the individual to whom the information relates.

J. Security and Maintenance

1. The **[name of entity and, if applicable, the name of entity's LPR vendor]** will operate in a secure facility protected from external intrusion and will utilize secure internal and external safeguards against network intrusions. Access to **[name of entity]** LPR information from outside the facility will be allowed only over secure networks.

2. All LPR equipment, software, and components will be properly maintained in accordance with the manufacturer's recommendations and/or any published industry standards.

3. The **[name of entity or, if applicable, the name of entity's LPR vendor]** will store LPR information in a manner that ensures that it cannot be added to, modified, accessed, or purged except by personnel authorized to take such actions.

4. Access to **[name of entity]** LPR information will be granted only to personnel whose positions and job duties require such access and who have successfully completed a background check and training.

5. Usernames and passwords to LPR information are not transferrable, must not be shared by **[name of entity]** personnel, and must be kept confidential.

6. User passwords must meet the following standards **[insert rules, such as no English words and a combination of letters, numbers, and at least two symbols]**. The system administrator will ensure that all manufacturer-generated default passwords are replaced with secure passwords before web-based interfaces of the system become operational.

7. Queries made to the **[name of entity]**'s LPR information will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit.

8. The **[name of entity]** will maintain an audit trail of accessed, requested, or disseminated **[name of entity]**-held LPR information. An audit trail will be kept for a minimum of **[specify the retention period for your jurisdiction/entity for this type of request]** of requests for access to LPR information for specific purposes and of what LPR information is disseminated to each individual in response to the request. Audit logs will include:

   - The name and agency of the law enforcement user.
   - The date and time of access.
   - The specific information accessed.
   - The modification or deletion, if any, of the LPR information.
   - The authorized law enforcement or public safety justification for access, including a relevant case number if available.

9. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

10. **Option 1: State Information Breach Law**

    The **[name of entity]** will follow the information breach notification guidance set forth in **[cite to applicable law]**. **[To the extent required by the (state) information breach notification law, add:]** The **[name of entity]** will immediately notify the originating agency from which the **[name of entity]** received personal information of a suspected or confirmed breach of such information.

    Option 2: No State Information Breach Law

    A: Entity Follows Guidance From the Office of Management and Budget (OMB)
    The **[name of entity]** will follow the information breach notification guidance set forth in OMB Memorandum M-07-16 (May 2007), available at http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf.

    B: Entity Adheres to the Following Policy
    [If there is no applicable state information breach notification law.] The **[name of entity]** will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the individual. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or take any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

K. Information Retention and Purging

1. All LPR information contained within the **[name of entity]**'s LPR system will be stored for a period not to exceed **[insert a time frame]**. After **[insert time period]**, the information will be automatically purged (i.e., permanently removed from the system).

This retention policy applies only to the LPR information contained in the **[name of entity]**'s LPR system itself. Once an LPR record is downloaded by **[name of entity]** personnel and incorporated into a criminal intelligence record or investigative case file, the LPR information is then considered intelligence or investigative information and the laws, regulations, and policies applicable to that type of information or intelligence govern its use.

If the LPR record has become or there is reason to believe that it will become evidence, including evidence that tends to inculpate or exculpate a suspect, in a specific criminal or other law enforcement investigation or action, the following provisions apply:

a. In those circumstances in which an LPR record is identified as having evidentiary value, the LPR **[insert Administrator or other title]** or designee will review the facts of the specific case and determine whether the information should be retained beyond the established retention period. If it is determined that it is reasonable to believe the information has evidentiary value, the LPR **[insert Administrator or other title]** will authorize the transfer of the applicable record from the LPR system server to **[insert appropriate response; for example, "the entity's case management system" or "a form of digital storage media (CD, DVD, etc.) or other portable storage device"]**.
b. Agencies requiring LPR records to be retained by the **[name of entity]** beyond the established retention period may make a formal, written request to the **[name of entity]** to extend retention. Each request must specify the need for extended retention, the circumstances surrounding the request, the requesting agency's case number, and a specific point of contact within the requesting agency. The **[name of entity]** reserves the right to grant or deny agency requests based on the information provided.

The **[name of entity]** retains the right to remove LPR information earlier than the retention period, based on limitations of information storage requirements and subject to applicable statutory disclosure mandates. Early removal, however, will not be used as a means for intentionally interfering with a lawful complaint or a public records request. The retention period may be modified at any time by the **[name of entity]**, subject to applicable legal requirements.

L. Accountability and Enforcement

L.1. Transparency

1. The **[name of entity]** will be open with the public in regard to LPR information collection, receipt, access, use, dissemination, retention, and purging practices. The **[name of entity]**'s LPR policy will be made available in printed copy upon request and posted prominently on the **[name of entity]**'s Web site **[or Web page]** at **[insert Web address]**.

2. The **[name of entity]**'s **[Privacy Officer, LPR Administrator, or other position title]** will be responsible for receiving and responding to inquiries and complaints about incorrect information or privacy, civil rights, and civil liberties protections in the LPR information system maintained or accessed by the **[name of entity]**. The **[Privacy Officer, LPR Administrator, or other position title]** may be contacted at **[insert mailing address or e-mail address]**.

L.2. Accountability

1. The **[name of entity]** will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this LPR policy and applicable law. This will include logging access to LPR information and periodic random auditing of these systems, so as not to establish a discernable pattern that may influence users' actions. These audits will be mandated at least **[insert quarterly, semiannually, annually, or other time period]**, and a record of the audits will be maintained by the **[Privacy Officer, LPR Administrator, or title of designee]** of the **[name of entity]**. Audits may be completed by an independent third party or a designated representative of the **[name of entity]**.

Appropriate elements of this audit process and key audit outcomes will be compiled into a report and may be provided to command staff and oversight entities or governance boards.[4]

[Entities may also release the results of the audit to the public, pursuant to law or as a matter of discretion. Under these circumstances, consider the following options.]

Option 1: The **[name of entity]** will provide, at minimum, an overview to the public to enhance transparency with respect to privacy, civil rights, and civil liberties protections built into the **[name of entity]**'s operations.

Option 2: The **[name of entity]** will also release to the public the full audit, with redactions as necessary to protect the privacy of any individual or group, if appropriate and consistent with jurisdictional requirements.

2. The **[name of entity]**'s personnel or other authorized users shall report errors and suspected or confirmed violations of the **[name of entity]**'s LPR policy to the **[name of entity]**'s **[insert title of LPR Administrator]**.

3. The **[Privacy Officer, LPR Administrator, or other position title]** will review and update the provisions contained in this LPR policy annually and will make appropriate changes in response to changes in applicable law, technology, and/or the purpose and use of the LPR system; the audit review; and public expectations.

L.3. Enforcement

1. If **[name of entity]** personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, receipt, access, use, dissemination, retention, and purging, the **[title of entity Director]** of the **[name of entity]** will:

   - Suspend or discontinue access to information by the **[name of entity]** personnel, the participating agency, or the authorized user;
   - Apply appropriate disciplinary or administrative actions or sanctions;
   - If the authorized user is from an agency external to the **[name of entity]**, request that the user's employer initiate disciplinary proceedings to enforce the policy's provisions; and/or
   - Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

2. The **[name of entity]** reserves the right to establish the qualifications and number of personnel having access to **[name of entity]** LPR information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating this LPR policy.

M. Training

1. Before access to **[name of entity]** LPR information is authorized, the **[name of entity]** will require the following individuals to participate in training regarding implementation of and adherence to this LPR policy:

   - All authorized **[name of entity]** personnel.
   - All authorized participating agency personnel.
   - All authorized personnel providing information technology services to the **[name of entity]**.

2. The **[name of entity]**'s LPR policy training program will cover:

   - Purposes of the LPR policy.
   - Substance and intent of the provisions of this LPR policy, and any revisions thereto, relating to collection, receipt, access, use, dissemination, retention, and purging of the **[name of entity]**'s LPR information and the privacy, civil rights, and civil liberties protections on the use of the technology and the information collected or received.
   - Appropriate procedures relating to license plate image quality and mitigating the risks associated with a possible misread by the LPR system.
   - LPR verification process for law enforcement alerts.
   - Originating and participating agency responsibilities and obligations under applicable federal, state, or local law and policy.
   - How to implement the LPR policy in the day-to-day work of the user, whether a paper or systems user.
   - Mechanisms for reporting violations of **[name of entity]** LPR policy provisions.
   - The nature and possible penalties for LPR policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

[1] Refer to state law regarding ownership and compliance with open record requests regarding LPR information.

[2] For further information about these processes, see *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies* at 4, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/35/Recommendations-for-First-Amendment-Protected-Events-for-State-and-Local-Law-Enforcement-Agencies.
[3] Ibid. at 6–7 and 11–13.
[4] *Privacy, Civil Rights, and Civil Liberties Audit Guidance for the State, Local, Tribal, and Territorial Intelligence Component*, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/181/Privacy--Civil-Rights--and-Civil-Liberties-Audit-Guidance-for-the-State--Local--Tribal--and-Territorial-Intelligence-Component.