Indiana Intelligence Fusion Center

License Plate Reader Policy

June 1, 2022

The Indiana Intelligence Fusion Center License Plate Reader Policy represents the policy applicable to all IIFC operations and activities.

Purpose Statement

The mission of the Indiana Intelligence Fusion Center (IIFC) is to collect, evaluate, analyze, and disseminate information and intelligence data (records) regarding criminal and terrorist activity in the State of Indiana while protecting privacy, civil rights, civil liberties, and other protected interests. This includes implementing appropriate privacy and civil liberties safeguards as outlined in the principles of the Privacy Act of 1974, as amended, to ensure that the information privacy and other legal rights of individuals and organizations are protected The information and intelligence data collected, evaluated, and analyzed will be disseminated by the IIFC to members of the law enforcement and public safety communities responsible for the prevention, mitigation, and response to crime and terrorism.

The purpose of this privacy, civil rights, and civil liberties (P/CRCL) protection policy is to promote IIFC and user conduct that complies with applicable federal and state law and assists the center and its users in:

- Increasing public safety and improving national security.
- Minimizing the threat and risk of injury to specific individuals.
- Minimizing the threat and risk of physical or financial injury to law enforcement and others responsible for public protection, safety, or health.
- Minimizing the threat and risk of damage to real or personal property.
- Protecting individual privacy, civil rights, civil liberties, and other protected interests.
- Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information.
- Minimizing the reluctance of individuals or groups to use or cooperate with the justice system.
- Supporting the role of the justice system in society.
- Promoting governmental legitimacy and accountability.
- Not unduly burdening the ongoing business of the justice system.
- Making the most effective use of public resources allocated to public safety agencies.

The IIFC recognizes the importance of ensuring the protection of individual constitutional rights, civil liberties, civil rights, and privacy interests throughout the intelligence process.

The IIFC policy manual contains the standards the IIFC will adhere to for the collection, use, and security of intelligence and information, as well as accountability guidelines for the management of such intelligence or information.

This policy applies to LPR information collected or received, accessed, used, disseminated, retained, and purged by the IIFC or delegable agency.

The policy is applicable to all personnel working in direct support of the IIFC.

The information was not obtained in violation of applicable federal, state, or local laws or ordinances (delegable to a submitting agency).

An outside agency, or investigators from an outside agency, may request LPR searches to assist with investigations only if:

- The outside agency is a law enforcement agency or provides a law enforcement function that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in the IIFC Privacy Policy. The requestor shall provide their contact information (requestor's name, requestor's agency, address, and phone number), and lawful reason for request.

The IIFC will provide a printed or electronic copy of this LPR policy to all, via the IIFC website.

The IIFC requires all users of IIFC to be in compliance with the IIFC Privacy Policy and all laws and regulations.

Governance and Oversight

Primary responsibility for the operation of the IIFC, its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis destruction, sharing, or disclosure of information; and the enforcement of this policy is assigned to the Executive Director of the IIFC.

The Indiana Intelligence Fusion Center Executive Director will be responsible for the following**:**

- Overseeing and administering LPR program to ensure compliance with applicable laws, regulations, standards, and policy.

Personnel from the following agencies are authorized to request LPR searches:

- Any Federal, State, Local, Tribal or governmental agency acting in a law enforcement capacity and making a lawful request or providing a lawfully obtained image for LPR analysis under the guidelines of the IIFC Privacy Policy of this document.

The Indiana Intelligence Fusion Center contracts with Vigilant Solutions to provide software and system development services for the Indiana Intelligence Fusion Center LPR system.

IIFC privacy compliance is guided by a trained Privacy Officer who is appointed by the Executive Director. Violations of the privacy policy can be reported to, the Executive Director, Assistant Director or to the Privacy Officer. Reporting can be made in person, written or via any electronic communication.

Information

The Indiana intelligence fusion center may collect criminal intelligence information only if:

- Reasonable suspicion exists that the subject of the criminal intelligence information is involved with or has knowledge of possible criminal or terrorist activity; and
- The criminal intelligence information is relevant to the criminal or terrorist activity.

IIFC personnel are required to adhere to the ISE- SAR Functional Standard and state and federal law for the receipt, collection, assessment, storage, access, dissemination, retention, and security of Suspicious activity reporting (SAR) information.

The IIFC may retain information that is based on a level of suspicion that is reasonably indicative of pre-operational behavior such as tips and leads or suspicious activity report (SAR) information, as it pertains to terrorist, subject to the policies and procedures specified in this policy.

- The ISE-SAR Functional Standard *does not alter law enforcement officers' constitutional obligations when interacting with the public*. This means, for example, that constitutional protections and agency policies and procedures that apply to a law enforcement officer's authority to stop, stop and frisk ("Terry Stop"), request identification, or detain and question an individual apply in the same measure to observed behavior *that is reasonably indicative of pre-operational planning associated with terrorism*. It is also important to recognize that many terrorism-related activities are now being funded via local or regional criminal organizations whose direct association with terrorism *may be tenuous*. This places law enforcement and homeland security professionals in the unique, yet demanding, position of identifying suspicious behaviors *as a by-product or secondary element in a criminal enforcement or investigative activity*.

The IIFC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as constitutional rights, including personal privacy and other civil liberties, and civil rights.

The IIFC will not seek or retain, and information-originating agencies will agree not to submit, information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.

- When participating on a federal law enforcement task force or when documenting a SAR or an ISE-SAR in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity must not be considered as factors creating suspicion. However, those attributes may be documented in specific suspect descriptions for identification purposes.

The IIFC applies labels to agency-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:

- the information pertains to all individuals pursuant to IC 10-11-9-4, and
- The information is subject to Federal and Indiana state laws restricting access, use, or disclosure, including, but not limited to, 18 USC 2721, IC 35-38-9 et seq., IC 31-39-8 et seq., IC 4-1-10 et seq., IC 5-2 et seq., IC 5-14-3 et seq., and 28 CFR, Part 23.

IIFC personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency will assign categories to the information) to reflect the assessment, such as:

- Whether the information consists of tips and leads data, suspicious activity reports, criminal history or intelligence information, case records, conditions of supervision, or case progress, etc.;
- The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector);
- The reliability of the source (for example, reliable, usually reliable, unreliable, unknown); and
- The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

At the time a decision is made to retain information, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:

- Not interfere with or compromise pending criminal investigations;
- Protect an individual's right of privacy, civil rights, and civil liberties; and
- There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

The IIFC will identify and review information that is originated by the IIFC prior to sharing that information in the ISE.

The IIFC requires certain basic descriptive information to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure. The types of information should include:

- The name of the originating department, component, and subcomponent.
- The name of the agency's justice information system from which the information is disseminated.
- The date the information was collected and, where feasible, the date its accuracy was last verified.
- The title and contact information for the person to whom questions regarding the information should be directed.

The IIFC will attach (or ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

The IIFC will keep a record of the source of all information retained by the agency.

Acquiring and Receiving LPR Information

The IIFC will query database LPR information that:

- Reasonable suspicion exists that the subject of the criminal intelligence information is involved with or has knowledge of possible criminal or terrorist activity; and
- The criminal intelligence information is relevant to the criminal or terrorist activity.
- Or applicable state law

Hot-list information is information is only considered if it meets the requirements of the IIFC Privacy Policy and applicable state law.

The IIFC 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.

IIFC accessed LPR information contains images of license plates that may be 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.

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 IIFC 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 IIFC accesses may be the result of an LPR system's automated collection of license plate numbers, it is the investigation process that identifies individuals

The IIFC protects all LPR information as prescribed by law, regulation or Privacy Policy.

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

The IIFC 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.Use of LPR Information

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

Sharing and Dissemination of LPR Information

The Indiana Intelligence Fusion Centers (IIFC) LPR search 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 IIFC's agreement with the commercial vendor.
- Disclosed or published without prior notice to the originating entity that such information is subject to disclosure or publication. However, the IIFC and the originating agency may agree in writing in advance that the IIFC will disclose LPR search information as part of its normal operations, including disclosure to an external auditor of the LPR search information.
- Disclosed on a discretionary basis unless the originating agency has provided prior written approval or unless such disclosure is otherwise authorized by the MOU or agreement between the IIFC and the originating agency.
- Disclosed to unauthorized individuals or for unauthorized purposes.

Information Quality Assurance

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.

- The IIFC considers the results, if any, of an LPR search to be advisory in nature as an investigative lead only. LPR search results are not considered positive identification of a subject and do not, on their own, establish probable cause, without further investigation. Any possible connection or involvement of the subject(s) to the investigation must be determined through further investigative methods.

The IIFC will make every reasonable effort to perform routine maintenance, upgrades and enhancements, testing, and refreshes of the LPR system to ensure proper performance, including the following:

- Personnel shall assess the LPR system on a regular basis to ensure performance and accuracy.
- Malfunctions or deficiencies of the system will be reported to the Director of Operations upon discovery of the malfunctions or deficiencies.

The integrity of information depends on quality control and correction of recognized errors which is key to mitigating the potential risk of misidentification or inclusion of individuals in a possible identification. The IIFC will investigate, in a timely manner, alleged errors and malfunctions or deficiencies of LPR information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and malfunctions or deficiencies. The IIFC will correct the information or advise the process for obtaining correction of the information per the IIFC Privacy Policy.

Security and Maintenance

- The IIFC will comply with generally accepted industry or other applicable standards for security, in accordance with Indiana Office of Technology to protect data at rest, in motion, or in use. Security safeguards will cover any type of medium (printed or electronic) or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related IIFC activity.
- All entities to the project will operate in a secure environment protected with multiple layers of security from external intrusion and will utilize secure internal and external security and privacy safeguards against network intrusions, such as strong multifactor authentication; encrypted communications; firewalls; and other reasonable physical technological, administrative, procedural, and personnel security measures to minimize the risks of unauthorized access to the system. Any access to IIFC LPR information from outside the facility will be allowed only over secure networks.
- All results produced by the IIFC as a result of an LPR search are disseminated by secured electronic means (such as an official government e-mail address). Non-electronic disseminations will be conducted personally or by phone with the requestor or designee.
- All LPR software and components will be properly maintained in accordance with the manufacturer's recommendations, including routine updates as appropriate.
- The IIFC will store LPR information in a manner that ensures that it cannot be modified, accessed, or purged except by personnel authorized to take such actions.
- Authorized access to the IIFC LPR system will be granted only to personnel whose positions and job duties require such access.
- Usernames and passwords to the LPR system are not transferrable, must not be shared by IIFC personnel, and must be kept confidential. • Queries made to the IIFC's LPR system 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.
- The IIFC will maintain an audit trail of requested, accessed, searched, or disseminated IIFC held LPR information, via Vigilant Solutions. An audit trail will be kept for requests, access, and searches of LPR information for specific purposes and of what LPR information is disseminated to each individual in response to the request.

Information Retention and Purging

- Once an LPR image is downloaded by IIFC personnel and incorporated into a criminal intelligence record or an investigative case file, the LPR information is then considered criminal intelligence or investigative information, and the laws, regulations, and policies applicable to that type of information or criminal intelligence govern its use.
- Images provided by an agency will be considered lead information and retained per the IIFC privacy policy pertaining to lead information, until such time that the originating agency provides an update to IIFC.
- The IIFC retains the right to remove LPR images from the repository earlier than the retention period, based on the limitations of information storage requirements and subject to any applicable record retention laws and 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 IIFC subject to applicable legal requirements.
- LPR search results may be saved within the entity's system audit log for audit purposes only. The audit log is available only to the Executive Director, Assistant Director, Director of Operations and Director of Intelligence and Analysis. LPR searches cannot be performed using the audit log.

Accountability and Enforcement

- The IIFC will follow procedures and practices by which it can ensure and evaluate the compliance of users with the LPR system requirements and with the provisions of this policy and applicable law. This will include logging access to LPR information, may include any type of medium or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related activity, and will entail 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 annually, and a record of the audits will be maintained by the Privacy Officer, of the IIFC pursuant to the retention policy. Audits may be completed by an independent third party or a designated representative of the IIFC
- The Assistant Director**,** 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.

Enforcement

If IIFC 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 Executive Director of the IIFC will:

- Suspend or discontinue access to information by the IIFC entity personnel, the participating agency, or the authorized user.
- Apply appropriate disciplinary or administrative actions or sanctions.
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

(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.[1]

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.

[1] 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.[2] 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

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

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.[3]

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.[4]

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.[5]

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.
- 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.

[3] 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.

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

[5] Ibid.

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.[6] 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 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.[7]

Linkable Information—Information about or related to an individual for whom there is a possibility of logical association with other information about that individual.[8]

Linked Information—Information about or related to an individual that is logically associated with other information about that individual.[9]

---

[6] 6 Ibid.
[7] Ibid.
[8] Automated License Plate Recognition (ALPR), General Order 17.102, Tempe Police Department, Arizona, 12132003.
[9] Ibid.

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[10]—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.

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.

[10] Automated License Plate Recognition (ALPR), General Order 17.102, Tempe Police Department, Arizona, 12132003.

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