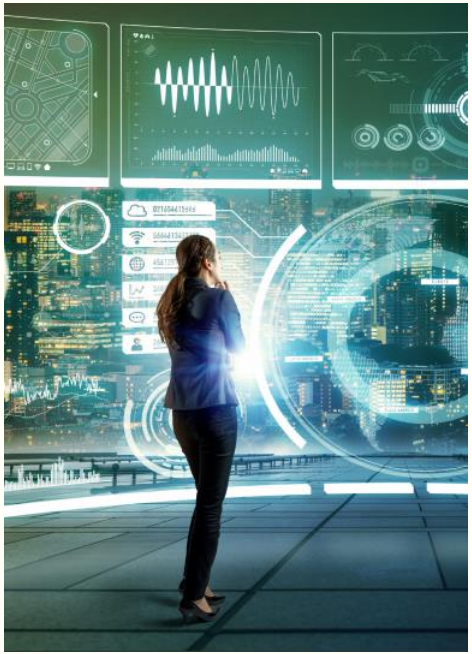
Utah Department of Public Safety

Statewide Information & Analysis Center

DPS Future Use of Automated License Plate Reader Systems

SIAC's Mission

"To serve Utah by providing innovative intelligence that advances response to public safety threats while protecting privacy rights for all."



Introduction

- The Utah Department of Public Safety's Use.
- Utah Legislature's Approval
- Utah Department of Transportation's permit process.

Benefits

- Stolen Vehicles
- Wanted Persons
- Amber Alerts and Missing Persons Cases
- Warrant Checks
- Investigative Tool
- Pattern Analysis
- Linking Vehicles to Crime Scenes
- Search for Persons of Interest
- Preventing and Investigating Terrorism

Privacy Concerns

- Invasion of Privacy
- Data Security
- Potential for Misuse
- Surveillance State

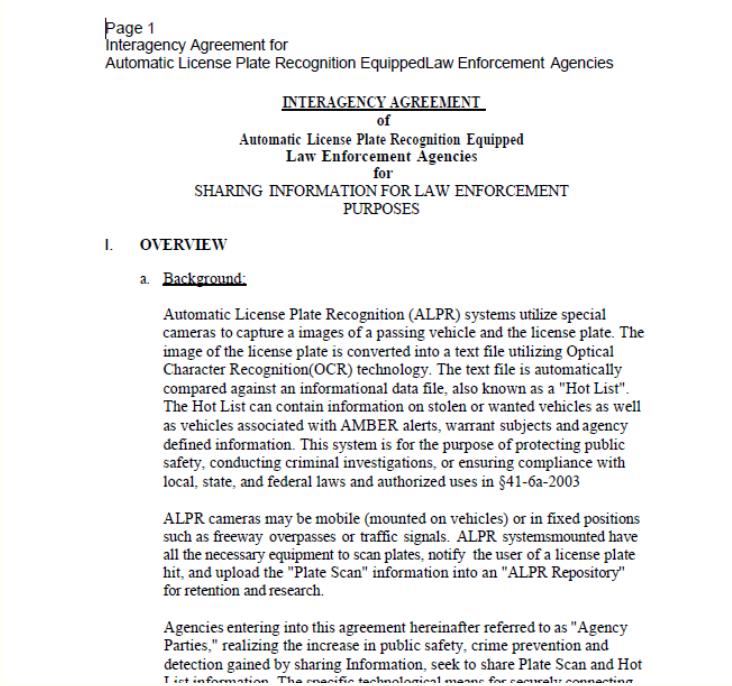
Statutory Authority, Legal Compliance, Governance and Oversight, Retention of Information, Classification of Information Regarding Validity of Reliability, Information Quality Assurance, Acquiring and Receiving Information, Merging of Information, Information sharing, dissemination, and Disclosure, Privacy Safeguards, Complaints and Corrections, Security Safeguards, Destruction of Information, Accountability, Enforcement, Training

Utah S.B. 250

- Allows UDOT to Provide Permits for Use
- Guardrails of Use and Implementation
- Requires an agency to maintain an ALPR Policy
- Requires an MOU for information Sharing
- Requires Collection and Retention for Auditing

Memorandums of Understanding (MOUs)

To date, 23 agencies have signed the DPS MOU.



Page 1
Interagency Agreement for
Automatic License Plate Recognition EquippedLaw Enforcement Agencies

INTERAGENCY AGREEMENT
of
Automatic License Plate Recognition Equipped
Law Enforcement Agencies
for
SHARING INFORMATION FOR LAW ENFORCEMENT
PURPOSES

I. **OVERVIEW**

a. Background:

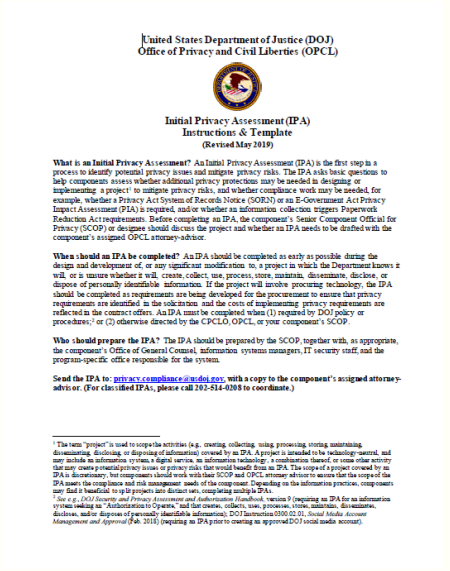
Automatic License Plate Recognition (ALPR) systems utilize special cameras to capture a images of a passing vehicle and the license plate. The image of the license plate is converted into a text file utilizing Optical Character Recognition(OCR) technology. The text file is automatically compared against an informational data file, also known as a "Hot List". The Hot List can contain information on stolen or wanted vehicles as well as vehicles associated with AMBER alerts, warrant subjects and agency defined information. This system is for the purpose of protecting public safety, conducting criminal investigations, or ensuring compliance with local, state, and federal laws and authorized uses in §41-6a-2003

ALPR cameras may be mobile (mounted on vehicles) or in fixed positions such as freeway overpasses or traffic signals. ALPR systemsmounted have all the necessary equipment to scan plates, notify the user of a license plate hit, and upload the "Plate Scan" information into an "ALPR Repository" for retention and research.

Agencies entering into this agreement hereinafter referred to as "Agency Parties," realizing the increase in public safety, crime prevention and detection gained by sharing Information, seek to share Plate Scan and Hot List information. The specific technological means for securely connecting

Privacy Impact Assessment Tool

- A proactive measure to evaluate and address privacy risks.
- Integrated into the decision-making process.



United States Department of Justice (DOJ)
Office of Privacy and Civil Liberties (OPCL)

Initial Privacy Assessment (IPA)
Instructions & Template
(Revised May 2019)

What is an Initial Privacy Assessment? An Initial Privacy Assessment (IPA) is the first step in a process to identify potential privacy issues and mitigate privacy risks. The IPA asks basic questions to help components assess whether additional privacy protections may be needed in designing or implementing a project[1] to mitigate privacy risks, and whether compliance work may be needed, for example, whether a Privacy Act System of Records Notice (SORN) or an E-Government Act Privacy Impact Assessment (PIA) is required, and/or whether an information collection triggers Paperwork Reduction Act requirements. Before completing an IPA, the component's Senior Component Official for Privacy (SCOP) or designee should discuss the project and whether an IPA needs to be drafted with the component's assigned OPCL attorney-advisor.

When should an IPA be completed? An IPA should be completed as early as possible during the design and development of, or any significant modification to, a project in which the Department knows it will, or is unsure whether it will, create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information. If the project will involve procuring technology, the IPA should be completed as requirements are being developed for the procurement to ensure that privacy requirements are identified in the solicitation and the costs of implementing privacy requirements are reflected in the contract offers. An IPA must be completed when (1) required by DOJ policy or procedures;[2] or (2) otherwise directed by the CPCLO, OPCL, or your component's SCOP.

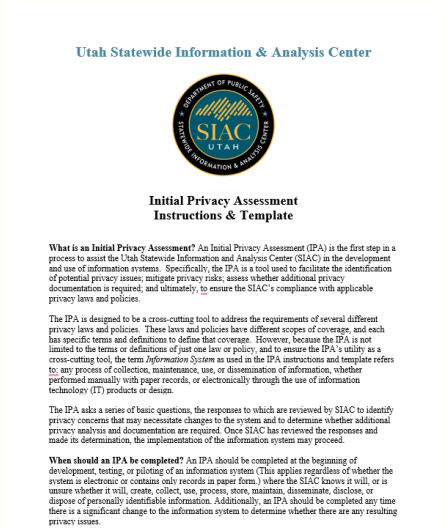
Who should prepare the IPA? The IPA should be prepared by the SCOP, together with, as appropriate, the component's Office of General Counsel, information systems managers, IT security staff, and the program-specific office responsible for the system.

Send the IPA to: privacy.compliance@usdoj.gov, with a copy to the component's assigned attorney-advisor. (For classified IPAs, please call 202-514-0208 to coordinate.)

[1] The term "project" is used to scope the activities (e.g., creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, or disposing of information) covered by an IPA. A project is intended to be technology-neutral, and may include an information system, a digital service, an information technology, a combination thereof, or some other activity that may create potential privacy issues or privacy risks that would benefit from an IPA. The scope of a project covered by an IPA is discretionary, but components should work with their SCOP and OPCL attorney advisor to ensure that the scope of the IPA meets the compliance and risk management needs of the component. Depending on the information practices, components may find it beneficial to split projects into distinct sets, completing multiple IPAs.

[2] *See e.g.*, *DOJ Security and Privacy Assessment and Authorization Handbook*, version 9 (requiring an IPA for an information system seeking an "Authorization to Operate," and that creates, collects, uses, processes, stores, maintains, disseminates, discloses, and/or disposes of personally identifiable information); DOJ Instruction 0300.02.01, *Social Media Account Management and Approval* (Feb. 2018) (requiring an IPA prior to creating an approved DOJ social media account).

- **Scope Definition**
- **Data Mapping**
- **Risk Identification**
- **Privacy Principles and Legal Compliance**
- **Mitigation Strategies**
- **Documentation and Reporting**
- **Stakeholder Engagement**
- **Monitoring and Review**
- **Decision-making Support**
- **Transparency and Accountability**



Utah Statewide Information & Analysis Center

Initial Privacy Assessment
Instructions & Template

What is an Initial Privacy Assessment? An Initial Privacy Assessment (IPA) is the first step in a process to assist the Utah Statewide Information and Analysis Center (SIAC) in the development and use of information systems. Specifically, the IPA is a tool used to facilitate the identification of potential privacy issues; mitigate privacy risks; assess whether additional privacy documentation is required; and ultimately, to ensure the SIAC's compliance with applicable privacy laws and policies.

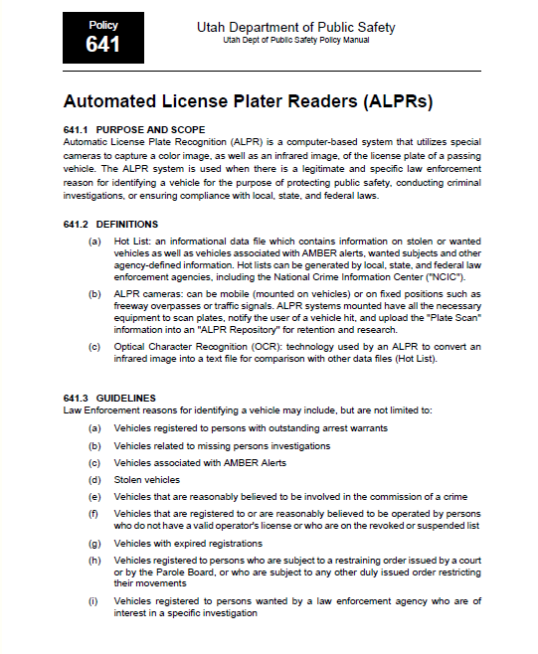
The IPA is designed to be a cross-cutting tool to address the requirements of several different privacy laws and policies. These laws and policies have different scopes of coverage, and each has specific terms and definitions to define that coverage. However, because the IPA is not limited to the terms or definitions of just one law or policy, and to ensure the IPA's utility as a cross-cutting tool, the term *Information System* as used in the IPA instructions and template refers to: any process of collection, maintenance, use, or dissemination of information, whether performed manually with paper records, or electronically through the use of information technology (IT) products or design.

The IPA asks a series of basic questions, the responses to which are reviewed by SIAC to identify privacy concerns that may necessitate changes to the system and to determine whether additional privacy analysis and documentation are required. Once SIAC has reviewed the responses and made its determination, the implementation of the information system may proceed.

When should an IPA be completed? An IPA should be completed at the beginning of development, testing, or piloting of an information system (This applies regardless of whether the system is electronic or contains only records in paper form.) where the SIAC knows it will, or is unsure whether it will, create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information. Additionally, an IPA should be completed any time there is a significant change to the information system to determine whether there are any resulting privacy issues.

DPS ALPR & Privacy Policy

- Statutory Authority
- Legal Compliance
- Definitions
- Guidelines
- Data Collection and Verification
- Data Access and Security
- Retention and Privacy
- Quality Assurance
- Receiving Information
- Information Sharing
- Security Safeguards
- Accoutnability



Policy 641

Utah Department of Public Safety
Utah Dept of Public Safety Policy Manual

Automated License Plater Readers (ALPRs)

641.1 PURPOSE AND SCOPE
Automatic License Plate Recognition (ALPR) is a computer-based system that utilizes special cameras to capture a color image, as well as an infrared image, of the license plate of a passing vehicle. The ALPR system is used when there is a legitimate and specific law enforcement reason for identifying a vehicle for the purpose of protecting public safety, conducting criminal investigations, or ensuring compliance with local, state, and federal laws.

641.2 DEFINITIONS

(a) Hot List: an informational data file which contains information on stolen or wanted vehicles as well as vehicles associated with AMBER alerts, wanted subjects and other agency-defined information. Hot lists can be generated by local, state, and federal law enforcement agencies, including the National Crime Information Center ("NCIC").

(b) ALPR cameras: can be mobile (mounted on vehicles) or on fixed positions such as freeway overpasses or traffic signals. ALPR systems mounted have all the necessary equipment to scan plates, notify the user of a vehicle hit, and upload the "Plate Scan" information into an "ALPR Repository" for retention and research.

(c) Optical Character Recognition (OCR): technology used by an ALPR to convert an infrared image into a text file for comparison with other data files (Hot List).

641.3 GUIDELINES
Law Enforcement reasons for identifying a vehicle may include, but are not limited to:

(a) Vehicles registered to persons with outstanding arrest warrants

(b) Vehicles related to missing persons investigations

(c) Vehicles associated with AMBER Alerts

(d) Stolen vehicles

(e) Vehicles that are reasonably believed to be involved in the commission of a crime

(f) Vehicles that are registered to or are reasonably believed to be operated by persons who do not have a valid operator's license or who are on the revoked or suspended list

(g) Vehicles with expired registrations

(h) Vehicles registered to persons who are subject to a restraining order issued by a court or by the Parole Board, or who are subject to any other duly issued order restricting their movements

(i) Vehicles registered to persons wanted by a law enforcement agency who are of interest in a specific investigation

Internal Reviews & Audits Oversight

- Internal SIAC Privacy Officer Reviews
- Annual Internal DPS Audit
- Utah BCI TAC Audits

Oversight, Governance, and Transparency

- SIAC Governance Board
- External Stakeholder Visits

2022 SIAC Board Members

- The Commissioner of Public Safety **Commissioner Jess Anderson**
- The Deputy Commissioner of Public Safety **Jimmy Higgs**
- City of the first or second class: **Chief Jeff Carr-South Jordan PD**
- The Special Agent in Charge of the Federal Bureau of Investigation: **SAC Dennis Rice**
- The United States Attorney for the District of Utah: **US Attorney Trina Higgins**
- The Homeland Security Director for the State of Utah: **Acting ASAC-Brandon Crane**
- Representative of the Utah Sheriffs Association: **Sheriff Chad Jensen-Cache S.O.**
- County having a population of 100,000 or more: **Sherriff Kelly Sparks**
- County having a population of less than 100,000: **Sheriff Glover-Kane County S.O.**
- Representative of the Utah Chiefs of Police Association: **Chief Ken Wallentine**
- City of the third, fourth, or fifth class or town: **Darin Adams Cedar City**
- Four at-large members:
  - **Utah Representative Jefferson S. Burton**
  - **Utah Senator Derrin R. Owens**
  - **Dominion Energy – Matt Miller**
  - **Vivint Arena - Blake Paris**

Questions?