MEMORANDUM OF UNDERSTANDING

Between the

California Highway Patrol

and

Oakland Police Department

SUPERSEDES
This Memorandum of Understanding (MOU) is made and entered into as of _____ supersedes any existing MOUs in place between the listed organizations for the purposes described herein.

INTRODUCTION
The purpose of this MOU is to establish a standard agreement between the California Highway Patrol (CHP) and Oakland Police Department regarding the development, management, operation, and security of data exchanged between organizations as mutually beneficial.

AUTHORITY
The datasets (listed in background section) which Oakland Police Department will be submitting to CHP as part of this agreement is governed by California Vehicle Code 20008-20012 et seq., and other federal and state laws as appropriate.

BACKGROUND
Oakland Police Department seeks the cooperation of the CHP to participate in the electronic exchange of CHP 555 form data, replacing the need to exchange paper forms. The parties enter this MOU to expedite the processing of data critical to both organizations in the furtherance of motor vehicle and highway safety.

COMMUNICATIONS
Frequent formal communications are essential to ensure the successful management and operation of the established interconnections. Both organizations agree to maintain open lines of communications between designated staff at both the managerial and technical levels. Critical communications described herein must be conducted in writing unless otherwise noted. The principal contacts for this MOU are as detailed below:

California Highway Patrol	Oakland Police Department
Josh Ehlers, Chief	<Contact Name>
Chief Information Officer (CIO) Information Management Division	<Title> <Organization>
601 North 7th Street Sacramento, CA 95811	<Street Address> <City State Zip>
Phone: (916) 843-4000	<Phone Number>
JEhlers@chp.ca.gov	<E-mail address>

Both organizations agree to designate and provide contact information for technical leads for their respective system, and to facilitate direct communication between technical leads to support the management and operation of the interconnection. If applicable, to safeguard the confidentiality, integrity, and availability of the interconnected systems; as well as the data they store, process, and send; the organizations agree to give notice of specific events within the time frames indicated below:

- **SECURITY INCIDENTS**
  Both organizations agree to notify the appropriate designee by telephone or e-mail at the earliest opportunity in the event a security incident impacting this data exchange agreement has been detected, so the other organization may take steps to determine whether its system has been compromised and to take appropriate security precautions. This communication should include a description of the incident, as well as the status of containment and/or resolution efforts. The system owner will receive a formal written incident summary within ten (10) business days of incident remediation.

- **DISASTERS AND OTHER CONTINGENCIES**
  Both organizations agree to provide notification to the appropriate designee by telephone or e-mail as they are reasonably able to in the event of a disaster, or other incident that impacts this data exchange agreement. This communication should include the cause of the outage and reasonable forecasts pertinent to the restoration of services. The system owner will receive a formal written event summary within ten (10) business days of restoration of services.

- **MATERIAL CHANGES TO SYSTEM CONFIGURATION**
  Planned technical changes to the system architecture that introduce either significant changes or new residual risk to the overall security posture of the system will be reported to technical staff before such changes are implemented. If the changes are determined to

negatively impact the terms of the MOU, the initiating party agrees to conduct a risk assessment and prepare an appropriately modified MOU within one (1) month of implementation for review. If planned changes will cause a disruption in service, notification shall be made no less than one (1) week in advance.

- **NEW INTERCONNECTIONS**
  Both organizations agree to ensure that information security safeguards are maintained with respect to the data exchanged under this agreement; to include any connection between its Information Technology (IT) system and any other IT system, including systems that are owned and operated by third parties.

- **PERSONNEL CHANGES**
  Both organizations shall allocate the appropriate personnel resources to ensure the continual function of the interconnection governed by this MOU, irrespective of changes in personnel. Both organizations agree to provide the other with notification of any changes in point of contact information.

INTERCONNECTION SECURITY AGREEMENT
This exchange is standard practice and does not require an interconnection security agreement.

SECURITY
Both organizations agree to work together to ensure the integrity of data they store, process, and transmit. Each organization certifies that its respective system is designed, managed, and operated in compliance with all relevant federal and state statutes, regulations, and policies pertaining to such systems.

- **DISCLOSURE**
  Both organizations agree not to disclose any information contained in records provided by the other organization which identifies, or can be used to identify, an individual person *except when used for the same statutorily authorized purpose for which it was received*. Consistent with California Civil Code Section 1798.29, this may include, but is not limited to, a person's name, driver's license number or identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual, account number or credit or debit card number (in combination with access credentials), medical information, health insurance information, unique biometric data (such as a fingerprint, retina, or iris image, used to authenticate a specific individual), information or data collected through the use or operation of an

automated license plate recognition system, or a username/e-mail address (in combination with access credentials).

- **APPROPRIATE USE**
  Both organizations agree not to use personal information from records provided by the other organization to contact or distribute bulk surveys, marketing, solicitations or for other purposes, unless the person whose information is used has provided express written consent for such disclosure.

- **LIMITATION OF USE**
  Both organizations agree not to provide any information from records obtained pursuant to this MOU to any other person without entering into an agreement including disclosure, appropriate use, and limitation of use identified herein.

- **PRIVACY PROTECTION**
  Both organizations agree to ensure that personnel are familiar with the provisions of the Driver Privacy Protection Act and adhere to federal laws and policies which protect personal identifying information in government records and systems, including the Privacy Act of 1974.

- **INVESTIGATIONS OF MISUSE/SECURITY BREACH**
  Both organizations agree to promptly investigate any alleged misuse of data or related security breach, and to cooperate reasonably with the appropriate personnel in connection with any alleged breaches involving its data.

Both organizations agree to respond to all requests by the other designed to ensure that each are adhering to the use and access limitations set forth in this agreement. Responses shall be in writing and shall be provided within ten (10) business days of receipt of the request.

COST CONSIDERATIONS

Unless otherwise specified, datasets will be provided via web service. Both organizations agree to incur any hardware/software/service costs necessary within their respective organization to establish and maintain a secure web service interconnection. Modifications to any system which are necessary to support an established interconnection are the responsibility of the respective system owner's organization.

TIMELINE

This agreement will remain in effect for five (5) years from the last date on either signature in the signature block below.

If both organizations wish to extend this agreement, they may do so by reviewing, updating, and reauthorizing this agreement. The newly signed agreement should explicitly supersede this agreement, which should be referenced by title and date.

If one or both of the parties wish to terminate this agreement, they may do so at any time and upon written 30-day advanced notice or immediately in the event of a security incident that necessitates a rapid response.

SIGNATORY AUTHORITY

The signatories below attest to having signing authority for the entities they represent and agree to the terms of this MOU.

Authorized Signatory on behalf of California Highway Patrol	Authorized Signatory on behalf of Oakland Police Department
Josh Ehlers Digitally signed by Josh Ehlers Date: 2026.05.04 15:15:17 -07'00'	
Signature	Signature Date
Josh Ehlers, Chief & CIO California Highway Patrol Information Management Division	<Authorizing Approver Information>