

06/20/2018

Ignition Interlock Program Guidelines for Manufacturers

Electronic Reporting Information

The Arizona Department of Transportation Ignition Interlock Program (The Department) utilizes an electronic automated reporting process. As required under A.R.S. §28-1461 and 17 A.A.C. 5, Articles 6 and 7, the certified ignition interlock device manufacturer must report information electronically in real time and in a form prescribed under A.R.S. §28-1461(B) to the Department. This information includes installations, compliance, calibrations, violations and removals as defined under A.R.S. §28-1301.

It is necessary to communicate directly with the manufacturers to ensure the Department receives and maintains current information. This information is exchanged between manufactures and the Department by means of a secured server environment.

Definitions:

As found - means data from the device before any maintenance is performed.

BrAC - means Breath Alcohol Content.

Calibration - means the testing, adjustment, or systematic standardization of an ignition interlock device to determine and verify its accuracy.

CIID - means Certified Ignition Interlock Device.

Circumvention - means the attempted or successful bypass of the proper functioning of a certified ignition interlock device, and includes the following;

- The operation of a vehicle without a properly functioning certified ignition interlock device;
- The push start (bump start) of a vehicle with a certified ignition interlock device;
- The introduction of a false sample other than a deep-lung breath sample from the person driving the vehicle;
- The introduction of an intentionally contaminated or a filtered breath sample;
- The intentional disruption or blocking of a digital image identification device;
- The continued operation of the vehicle with the certified ignition interlock device after the device detects excess breath alcohol; or
- When a person, who is required to maintain a functioning certified ignition interlock device is starting or operating the motor vehicle, permits another individual to breathe into the certified ignition interlock device for the purpose of providing a breath alcohol sample to start the motor vehicle or for the rolling retest.

Customer number - means the system-generated, or other distinguishing number, assigned by the Department to each person conducting business with the Department. The customer number of a private individual is generally the person's driver license or non-operating identification license number.

Drive cycle - means either the period of time from when a vehicle's ignition is initially turned on to the next time the ignition is turned off, or the period of time from when an initial breath alcohol test is performed and failed, to the time such test is successfully taken and the ignition is turned off.

FTP - means file transfer protocol, the exchange of files over any network that supports electronic data interchange reporting that is transmitted through the Internet and prescribed by the Department.

MPI or "manufacturer ID" - means Manufacture Provider Installer, this is the number assigned by the Department to each specific manufacture and its service centers. This number is used to identify each location for accurate reporting.

Ignition interlock period - means the period in which a person is required to use a certified ignition interlock device that is installed in a vehicle.

Tampering - means an overt or conscious attempt to physically disable, or otherwise disconnect the CIID from its power source that allows the operator to start the engine without taking and passing the requisite breath test.

Real-time or real-time reporting - means the instant transmission of unfiltered ignition interlock violations as defined in R17-5-601, and data as prescribed in R-17-5-610, including photos, to the manufacturer's website for viewing by the Department without delay, as electronic or digital service permits.

Violation reset - means the unplanned servicing and inspection of a certified ignition interlock device and the downloading of information from its data storage system by a service center as a result of an early recall that requires the manufacturer to unlock the device.

Background

Arizona Revised Statute §28-1461 requires the ignition interlock manufacturer to electronically report required data in real time from the CIID to the manufacturer's website as well as to send a daily FTP file through a secured server to the Department. All violations, including photographs, shall be available to the Department for viewing on the manufacturer's website within five minutes after the data is recorded on the device.

Each manufacturer participating in the Arizona Certified Ignition Interlock Device program is assigned its own personal directory on the Department secured server. The directory is used to receive and supply customer information and data captured by the CIIDs. Due to the nature of the environment, the information communicated back and forth with the Department is secure from the public, as well as, the other manufacturers.

Access is given to each manufacturer by way of private keys to the secured server. These keys are a combination of the manufacturer ID and the directory they are given access to. Access is only granted to two entities: the Department and the interlock manufacturers. Upon certification of the interlock device, the Department will request assistance from the ADOT Information Technology Group to create new manufacturer reporting codes in preparation for the electronic reporting testing phase.

The ADOT received data file (toadot.txt) is the reported file sent from the manufacturer to the Department daily. This file shall contain customer information and CIID data. The manufacturer reports to the Department when the device was installed and removed, who they installed it for, etc. The manufacturer's service centers are also required to check and maintain the devices throughout the entire ignition interlock period. The manufacturer sends the Department these results at the intervals specified by the requirement. This information includes the specifics of the compliance and calibration checks such as the location performed at, servicing technician, device numbers, etc. This file will also contain any violations received in real time by the manufacturer that day. Violations as prescribed by A.R.S. §28-1461 include tampering, circumvention, missed rolling retest violations, and BrAC violations.

The ADOT processed data file (fromadot.txt) is the return file containing information for each particular customer the manufacturer reported for in the ADOT received data (toadot.txt) file received for that day. The file includes records returned with errors (editing, not found, etc.).

The ADOT results data file (results.txt) also contains a recap of the data processed by the Department from the received data information file for that day. This allows the manufacturer to verify that all data has been transmitted successfully.

Physically how the process works:

In addition to systematically generating extensions and suspensions, the Department mainframe will systematically generate email notifications to the designated manufacturer email address every night after the manufacturer files are processed by the DI Auto program. The driver records are identified and attached to a 'note pad' document and attached to an email. The email notifications are separated into two categories and two separate email notifications. Each email will positively identify the driver by name and AZ customer number. Each email will also provide the associated docket number of the action listed.

toadot.txt – The manufacturer signs on their system and gains access to their own directory. They upload their daily performance file to the secured server. The Department retrieves that data at 8:00 pm daily. A scheduled mainframe job is executed MV326Gxx (xx = last two digits of the Manufacturer number). This job executes a process to copy the manufacturer's toadot.txt file from the SFTP server to the UNIX environment, and then deletes the file from the manufacturer's directory on the SFTP server. The deletion eliminates any duplicate data processing effort in the event the installer does not have a need to send files daily. A UNIX script is then executed that brings the information from the UNIX environment to the mainframe for storage and access by the Department to process.

fromadot.txt and results.txt – After the Department receives and processes the toadot.txt file, it is transmitted back to the manufacturer's directory for their review. It is a reverse process from the one stated above. A mainframe job is executed (MV326Pxx) that copies the mainframe file to the UNIX environment. When successful, a UNIX script copies the file from the UNIX environment to the secured server, where it is stored in the manufacturer's directory. This process replaces the file that was there from prior processing, so there is no need for a deletion step. Due to the returned information being replaced each day it is important that the manufacturer retrieves this file daily. The manufacturer shall review the file for error codes and initiates the appropriate action to ensure the Department has the correct information.

Note: The Department will transmit the fromadot.txt and results.txt files back to the manufacturer's directory even if the manufacturer's toadot.txt file is absent. In this situation the fromadot.txt file will be empty and the results.txt file will contain zeros. Manufacturers shall contact the Department immediately if a fromadot.txt or results.txt file has not been received for each days toadot.txt file. It is important that the manufacturer retrieves this file daily to review file error codes and initiate the appropriate action to ensure the Department has the correct information.

Each manufacturer will receive two email alerts each night following the toadot.txt, fromadot.txt, and results.txt process. The first email notification is labeled "**Adverse Conditions**". Adverse Conditions are defined as follows:

- **A01** - COMPLIANCE OR REMOVAL RECEIVED WITHOUT ANY PREVIOUS INSTALLATION NOTICE. Each manufacturer is expected to review the customer's file and verify the installation information and resend the install report to the Department in the next toadot.txt file sent, to assure proper reporting is being followed.
- **A02** - COMPLIANCE OR REMOVAL REPORT RECEIVED WHERE THE CUSTOMER HAS NOT YET REINSTATED. Each manufacturer is expected to refer the customers to MVD for proper action.
- **C13** - CUSTOMER PLACED ON NON-COMPLIANCE SUSPENSION. A C13 suspension will occur if a customer failed to come in for the required 90 day calibration appointment. Each manufacturer shall review the customer's history of calibration checks to ensure customer has maintained compliance (no missed appointments). If customer maintained compliance, (no missed appointments), the manufacturer is required to email IgnitionInterlock@azdot.gov with the date of calibration that was not received by the Department, as well as assure the same information is sent electronically in the next toadot.txt file sent. If the customer did not maintain compliance (missed appointment) no action is required on the manufacturer's behalf.

The second email notification is labeled "**Extensions for Review**". Extensions for review will provide the Name, AZ Customer Number, Docket # of Extension, and Reason Code and Definition of Extension.

- **C15** - CUSTOMER SERVED TAMPERING.
- **C16** - CUSTOMER SERVED BrAC VIOLATIONS EXTENSION.
- **C17** - CUSTOMER SERVED EXTENSION FOR BrAC VIOLATION WHILE CURRENTLY IN AN EXTENSION PERIOD.
- **C18** - CUSTOMER SERVED MISSED ROLLING RETEST VIOLATION.
- **C19** - CUSTOMER SERVED CIRCUMVENTION.

Expectations for “Extensions for Review”. The manufacturer is required to review each entry and verify the violation that caused the extension. After reviewing all of the information from the data loggers, photos, etc. the manufacturer shall notify the Department via email within 10 days if the violation is valid or not. Ten days after the Department receives the violation that caused the extension a notice will be mailed to the customer to notify them of the extension. This 10 day timeframe to validate extensions is crucial to ensure that customers do not receive invalid extensions. If the extension is valid the customers are given 15 days from the date of the notice sent by the Department to request a hearing.

1. If the violation that caused the extension is invalid, the manufacturer shall send a separate email to (IgnitionInterlock@azdot.gov) requesting to void the action with the subject header identifying the driver by name, customer number, date of birth, and docket #.
 - Attach any proof that the violation is invalid (data logger, photos, repair receipts, etc.).
2. If the violation that caused the extension is valid, the manufacturer shall send a separate email to their designation resource mailbox (Ex: Manufacturer = 001, their designated resource mailbox is ILDATALOGGERS001@azdot.gov) with the subject header identifying the driver by name, customer number, date of birth, and docket #. The email must include:
 - A summary report stating why the data logger or any other evidence validates the violation, including any photographs of the person.
 - A data logger that shows at least 12 hours of data before and after the violation.

Example Subject Header:

“VIOLATION VALIDATION FIRST,MIDDLE,LAST D00012345 MMDDYYYY AAA01234”

Each manufacturer shall provide to the Department one email address where the email alerts will be sent to at the time of manufacturer certification. The designated email address is then entered in the Department’s mainframe (MDILTBL) by an interlock unit representative.

SSH (Secure Shell Protocol) / Secure FTP Server

The Department will supply an FTP server with the SSH protocol, running SFTP. A user logon and password is required, and will be distributed once assigned. Each manufacturer will be assigned a logon ID and password.

Certificates

As a further step to ensure data security, each manufacturer and the Department will share their public keys. By using these certificates, even the logon ID and password are encrypted in transmission.

SSH / Secure FTP Transmission

Each manufacturer’s server should have the corresponding client side of SSH. Since this is a common protocol, most servers should already have this.

Process Flow

Manufacturers Data Submission

Format - See page 19 “Certified Ignition Interlock Device Summarized Reporting Record Layout”

Naming Conventions:

1. Incoming file to the Department’s server: toadot.txt.
2. Return file to manufacturers: Results file available for retrieval the following business day: fromadot.txt and results.txt

Schedule

Manufacturers may submit their files at any time during the day. The merge script on the Department’s server will run once per day, at 8:00 pm, each night Monday through Sunday, (regardless of holidays) collecting all entries submitted from all manufacturers for that day.

As the Department’s server that collects the ‘toadot’ files runs daily (regardless of holidays) the ADOT DI Auto program that creates the proper extensions and suspensions does not. This process runs Sunday through Friday (and does not run on holidays). This is important because if a manufacturer sends a file on Friday, Saturday and Sunday, their email alert notifications for Saturday will be added to the notifications sent on Sunday.

Example:

Friday manufacturer 001 sends extensions for 15 customers in the toadot.txt. file. Friday night they will receive 15 entries in the “Extensions for Review” alert email.

Saturday manufacturer 001 sends extensions for 7 customers in the toadot.txt. file. They will not receive any alert emails because DI Auto has not processed this file.

Sunday manufacturer 001 sends extensions for 10 customers in the toadot.txt. file. Sunday night they will receive 17 entries in the “Extensions for Review” alert email (Saturday and Sunday reports will be combined).

Note: If no extensions are found in the toadot.txt. file, an email alert will still be created and be sent to the designated email address, but will contain a blank attachment.

MVD Pull of Manufacturer’s Transmitted File

Each evening, the Department will get the toadot.txt file from each directory on the SFTP server. A process on the mainframe then merges all separate files into a single, sorted file and processes the results against the Department ignition interlock requirements databases.

MVD Processing

Return Exceptions

The “Certified Ignition Interlock Device Summarized Reporting Record” contains a specific position field holding a two-character error return code (position # 163 and 164). Every record sent by the manufacturer that evening is returned in the fromadot.txt file. The only exception to this is when the file is so corrupt, it is impossible to discern which manufacturer transmitted the file. The Department may add extra records to the return file when the customer reinstates their license. The Department will then return the entry with a “00” return code and the Department uninstall date populated.

Table #1 CIID Exception/Process Return Codes and Their Meaning:

Return Code	Reason	Action
00	Process successful	None unless it is an extra record returned by the Department, then use the MVD Uninstall Date as per your system requirements.
01	MPI not found or MPI not authorized	Verify 9-digit MPI is authorized by the Department. Manufacturer - Ensure correct MPI and resend data. Contact the Department for correct MPI.
02	Customer not found or Multiple hits found	Manufacturer - Ensure name, DOB, and licenses are correct and resend data.
03	Not Interlock Eligible	This driver has a Special Ignition Interlock Restricted Driver License (SIIRD), but the SIIRD has been cancelled. The Department – Review, correct and contact driver as needed.
41	Last Name contains invalid characters	Name field may only contain alphabetic characters, blanks or hyphens. Manufacturer – Ensure information is correct and resend data.

42	First Name contains invalid characters	<p>Name field may only contain alphabetic characters, blanks or hyphens.</p> <p>Manufacturer – Ensure information is correct and resend data.</p>
43	Middle Name contains invalid characters	<p>Name field may only contain alphabetic characters, blanks or hyphens.</p> <p>Manufacturer – Ensure information is correct and resend data.</p>
44	Customer (or DL) Number is invalid	<p>Customer Number may only contain alphanumeric characters.</p> <p>Manufacturer – Ensure information is correct and resend data.</p>
45	Date of Birth is invalid	<p>Date of Birth is required and must be a valid date in YYYYMMDD format</p> <p>Manufacturer – Ensure information is correct and resend data.</p>
04	Other Record Edit Error	<p>A required field is missing, or a required date field is in an invalid format. All date fields must be in YYYYMMDD format.</p> <p>Manufacturer – Ensure information is correct and resend data.</p>
05	No Active Requirement Found	<p>All interlock requirements have subsequently been voided by the courts.</p> <p>The Department – Review, correct and contact driver as needed.</p>

06	All Requirements Are Met	<p>Customer is no longer required to carry a CIID according to the Department records.</p> <p>Manufacturer - Have the driver contact the Department. If requirement has ended verify that a removal type "R" has been submitted.</p>
07	Duplicate Found on the Department records	<p>Data being transmitted already on customer record. Check daily files to determine if new files are being created to determine the reason for a duplicate found.</p> <p>The Department – Review, correct and contact driver as needed.</p>
08	CDL License and no Active SIIDL Requirement found	<p>Indicates that while the Department is receiving compliance reports, not all components which make them eligible for the SIIRDL are present in the Department system.</p> <p>The Department – Review, correct and contact driver as needed.</p>
09	SIIRDL found, but uninstall date is zeros in the Department system.	

Business Rules

The following customer data will be required for successful transmission:

Customer Data	Required /Optional Field	Manufacturer/The Department Transmission
Manufacturer ID	Required	Manufacturer
Provider ID	Required	Manufacturer
Installer ID	Required	Manufacturer
Last Name	Required	Manufacturer
First Name	Required	Manufacturer
Middle Name	Required	Manufacturer
DOB (YYYYMMDD)	Required	Manufacturer
DL/Customer #	Required	Manufacturer
Install Date (YYYYMMDD)	Required for report type I	Manufacturer
MVD Uninstall Date (YYYYMMDD)	Optional	The Department - Will provide to manufacturer when customer is no longer required to maintain IL.
Removal Date	Required for report type R	Manufacturer
Report Type: I = Installed C = Compliance check R = CIID Removed N = Non Compliance A = Calibration V = Violation E = Exchanged Unit M = Missing Device	Required (Must be I, C, R, A, V, E, M) The N type no longer used for new device reporting.	Manufacturer
Non-Compliance Code	Optional The NC field no longer used for new device reporting.	Manufacturer

BAC Violation Count	Optional Above the set point or higher for anyone under 21 years of age. .08% or higher for anyone over 21.	Manufacturer
Returned Error Code	Optional	The Department
Device Download Date (YYYYMMDD)	Required	Manufacturer
Device Download Time (HH:MM:SS:HS)	Required	Manufacturer
Tampering/Circumvention occurrence date	Optional	Manufacturer
BAC Violation Date 1	Required if the BAC count is 1, otherwise optional.	Manufacturer
BAC Violation Date 2	Required if the BAC count is 2, otherwise optional.	Manufacturer
BAC Violation Date 3	Required if the BAC count is 3 or more, otherwise optional.	Manufacturer
Device ID This is the number on the hand held device.	Optional	Manufacturer
Employee ID (Tech_ID) The department will assign each technician an ID number at the time of their certification.	Optional	Manufacturer
Bypass Approval	Required if a bypass was issued (Can be Y or blank).	Manufacturer

Bypass Time (HH:MM:SS:HS)	Required if bypass approval = Y.	Manufacturer
VIN – Last 6 digits of the vehicle VIN number the device is installed on.	Optional	Manufacturer
Interlock Order: C = Court Ordered M = MVD Ordered O = Other/Out of State More than one ordering agency may be reported. Example: “COM” for court, out of state, and MVD or “CM” for court and MVD.	Optional	Manufacturer
BAC Violation Time 1	Required if the BAC count is 1, otherwise optional.	Manufacturer
BAC Violation Value 1	Required if the BAC count is 1, otherwise optional.	Manufacturer
BAC Violation Time 2	Required if the BAC count is 2, otherwise optional.	Manufacturer
BAC Violation Value 2	Required if the BAC count is 2, otherwise optional.	Manufacturer
BAC Violation Time 3	Required if the BAC count is 3 or more, otherwise optional.	Manufacturer
BAC Violation Value 3	Required if the BAC count is 3 or more, otherwise optional.	Manufacturer
Tampering Violation Count	Optional	Manufacturer

Tampering Violation Time 1	Required if the tampering count is 1, otherwise optional.	Manufacturer
Tampering Violation Time 2	Required if the tampering count is 2 or more, otherwise optional.	Manufacturer
Circumvention Violation Count	Optional	Manufacturer
Circumvention Violation Time 1	Required if the circumvention violation count is 1, otherwise optional.	Manufacturer
Circumvention Violation Time 2	Required if the circumvention violation count is 2 or more, otherwise optional.	Manufacturer
Missed Rolling Retest Count	Optional Count of how many violations (3 consecutive missed rolling retests = 1 violation)	Manufacturer
Missed Rolling Retest Time 1	Required if the missed rolling retest count is 1, otherwise optional.	Manufacturer
Missed Rolling Retest Time 2	Required if the missed rolling retest count is 1, otherwise optional.	Manufacturer
Missed Rolling Retest Time 3	Required if the missed rolling retest count is 1, otherwise optional.	Manufacturer

Missed Rolling Retest Time 4	Required if the missed rolling retest count is 2 or more, otherwise optional.	Manufacturer
Missed Rolling Retest Time 5	Required if the missed rolling retest count is 2 or more, otherwise optional.	Manufacturer
Missed Rolling Retest Time 6	Required if the missed rolling retest count is 2 or more, otherwise optional.	Manufacturer
Send as received	Optional	Manufacturer

Upon successful transmission of the customer's installation date, the driver's record will be updated as follows:

1. Report type I is used for Installations.
2. The system will add install comment to the driver's record comment segment. The comment segment will display the following data:
Interlock Verified Installed on (date of install), by (MPI number)

Upon successful transmission of the customer's compliance check (30 and 60 days) the driver's record will be updated as follows:

1. Report type C is used for a Compliance check.
2. The system will update the driver's ignition interlock requirement record for the next required compliance and/or calibration interval.

Upon successful transmission of the customer's calibration date (77-90 days after install and every 77-90 days thereafter) the driver's record will be updated as follows:

1. Report type A is used for a Calibration.
2. The system will update the driver's ignition interlock requirement record for the next required calibration interval.

Upon successful transmission of the customer's tampering violation the driver's record will be updated as follows:

1. Report type V is used for a violation.
2. The system will add the count of how many tampering violations were reported.
3. The system will add the reported times in HR:MM:SS:HS format of the first two tampering violations reported in that file.
4. The system will add the tampering violation formatted comment. The system will review the current driver status and initiate required C15 extension(s).

Upon successful transmission of the customer's BrAC violation the driver's record will be updated as follows:

1. Report type V is used for a violation.
2. The system will add the count of how many BrAC violations were reported.
3. The system will add the reported dates and times in HR:MM:SS:HS format of the first three BrAC violations reported in that file.
4. Along with the times of the violations the system will add the correlating reported BrAC readings in ### format (Ex: The customer blows a .082 the manufacturer will report as 082).
5. The system will add the BrAC violation formatted comment. The system will review the current driver status and initiate required C16 extension(s).

Upon successful transmission of the customer's missed rolling retest violation the driver's record will be updated as follows:

1. Report type V is used for a violation.
2. The system will add the count of how many missed rolling retest violations were reported (Three consecutive missed rolling retests = One violation).
3. The system will add the reported times in HR:MM:SS:HS format of each of the missed test for the first two violations reported in that file. Six times total, 3 times for each of the first two violations.
4. The system will add the missed rolling retest violation formatted comment. The system will review the current driver status and initiate required C18 extension(s).

Upon successful transmission of the customer's circumvention violation the driver's record will be updated as follows:

1. Report type V is used for a violation.
2. The system will add the count of how many circumvention violations were reported.
3. The system will add the reported times in HR:MM:SS:HS format of the first two circumvention violations reported in that file.
4. The system will add the circumvention violation formatted comment. The system will review the current driver status and initiate required C19 extension(s).

Upon successful transmission of the customer's device exchange date the driver's record will be updated as follows:

1. Report type E is used for an exchange.
2. The system will add the new reported device number.

Upon successful transmission of the customer's missing device date the driver's record will be updated as follows:

1. Report type M is used for a missing device (after a customer fails to return for appointments and is unable to be contacted the manufacturer can report as a missing device).

Upon successful transmission of the customer's removal date the driver's record will be updated as follows:

1. The report type R is used for a Removal.
2. The system will log this data in the driver's record and no action will be necessary. If the customer has removed early and still has remaining time on the ignition interlock requirement, the customer is allowed 72 hours to complete another install or will be placed under a C14 suspension.

Reporting Requirements

Manufacturers receive a 9 digit reporting code called an MPI number from the Department upon certification for each of its service centers. This MPI number is specific to the service center it's assigned to. The manufacturer is required to report the data received from each service center under their assigned number only. All services including installs, removals, calibrations, and exchanges conducted at a service center are to be reported within 24 hours under the MPI number assigned to that service center, along with the technician ID assigned to the technician that conducted the services.

Manufacturers will also be assigned an MPI number to report all real time electronically received and sent data (violations and compliance checks) as well as another to report all out of state received data.

All violations will be reported in real time via electronic or digital service from the CIID to the manufacturer's website including 12 hours before and after the violation. The manufacturer shall then report that data in that days FTP file (toadot.txt) to the Department within 24 hours of the manufacturer receiving the data from the CIID.

Compliance checks:

- Compliance checks are electronic reports that do not require the customer to return to a service center. Compliance checks are to be sent at 30 and 60 days after the customers interlock requirement has begun (after reinstatement). This is needed for deferment eligibility. The following steps are needed in order for the manufacturer to comply with the 30 and 60 day after reinstatement schedule.
 - Thirty days after the customer's installation, send a compliance check.
 - If the compliance check is returned with an A02 adverse condition (**A02** - compliance or removal report received where the customer has not yet reinstated) then another compliance check must be resent every 30 days until the A02 adverse condition is not received. Once the A02 adverse condition is no longer received that indicates the customer has reinstated. The first compliance check sent without receiving an A02 will satisfy the 30 day requirement. After that a second one will need to be sent 30 days later to satisfy the 60 day requirement.
 - If the first compliance check sent 30 days after install is sent and returned without an adverse condition, this will satisfy the 30 day requirement. Thirty days after that, a second one will need to satisfy the 60 day requirement.

Calibration report:

- Calibrations are to be performed every 77-90 days after the install. When the calibration report type "A" is received the Department's system will update the customer's driver ignition interlock requirement record for the next required calibration to be received 77-90 days later. It is important that the manufacturer only reports the calibration report type "A" only at the 77-90 days intervals to maintain the proper reporting schedule of the customer's interlock requirement.

Exchange:

- If a customer's device malfunctions and needs to be replaced the report type "E" will be used. Exchanges are limited to the replacement of the hand held unit on the same vehicle (the last six of the vin previously reported should not change). Exchanges exclude if the customer wishes to move the device to a new vehicle. A vehicle change shall be reported as a removal and then as an install reflecting the last six of the new vin. If an exchange is needed at the time of a calibration, the manufacturer will not need to report the exchange report type "E". The manufacturer will use the report type "A" and change the device ID on the file.

Tampering:

- Only one tampering violation can be reported per drive cycle. However there may be more than one violation per day. Example: The customer starts the vehicle at 12:00:00:00. A tampering report is transmitted at 12:15:00:00, 12:37:00:00, and 12:40:00:00. The customer reaches their destination and turns off the vehicle at 12:55:00:00. Only one tampering violation will be reported for this drive cycle. Later that day, the customer starts the vehicle at 18:00:00:00 and has a tampering report transmitted at 18:15:00:00 and turns off the vehicle at 18:20:00:00. This would be reported as a second tampering violation. That night the customer starts the vehicle at 21:00:00:00 and has a tampering report transmitted at 21:20:00:00 and turns off the vehicle at 22:00:02:00. This would be reported as a third tampering violation. The manufacturer shall report a tampering count of 3 with the times of the first 2 violations, 12:15:00:00 and 18:15:00:00.

Circumvention:

- Only one circumvention violation can be reported per drive cycle. Total number of circumvention violations for that day will be reported with the times for the first two circumvention violations (same process listed for tampering violations).

BrAC:

- Only one BrAC violation can be reported per drive cycle. Total number of BrAC violations for that day will be reported with the dates, times, and BrAC readings for the first two BrAC violations (same process listed for tampering violations).

Missed rolling retest:

- A missed rolling retest is when a customer does not give a breath sample in the allotted 6 minutes. This does not include if the customer gives a breath sample and fails. A missed rolling retest violation is when a customer fails to properly perform any set of three consecutive rolling retests that occur within an 18 minute timeframe during a drive cycle. Multiple missed rolling retest violations can be reported for the same drive cycle. Example: The customer starts the vehicle at 11:55:00:00. The device prompts them for a rolling retest at 12:00:00:00 to which they have six minutes till 12:06:00:00 to comply. The customer did not comply by 12:06:00:00 so the device will prompt for a second rolling retest from 12:06:00:00 till 12:12:00:00. The customer did not comply by 12:12:00:00 the device will prompt for a third rolling retest from 12:12:00:00 till 12:18:00:00. The customer did not comply by 12:18:00:00. This is one missed rolling retest violation. Each set of three consecutive rolling retests that occur within an 18 minute timeframe shall be reported as a violation. The count of the three consecutive rolling retests are confined to each drive cycle, meaning that with the given example if the customer had turned off the vehicle at 12:11:00:00 this would only have been two missed rolling retests and the count would stop with the ending of the drive cycle by turning off the vehicle. With the above example of three consecutive rolling retests the manufacturer would report one violation with the times of 12:06:00:00, 12:12:00:00, and 12:18:00:00.

Note: The Departments system will calculate the times given to ensure the proper six minute intervals. If the times reported are not in six minute intervals the entire customer record will be rejected and sent back to the manufacturer with an 04 error code. The manufacturer must review the error and resend the complete customer record in the next toadot.txt file sent to the Department.

Possible multi reporting examples:

From the date of install the customer has a tampering violation transmitted at day 70. The customer will enter an early recall from day 70-73 for a violation reset. The customer, as instructed, returns to the service center to have the vehicle inspected and have the violation reset. This will be reported electronically in real time as a violation report type "V". However the department system still requires a calibration report type "A" to be performed and received at the 77-90 day interval. The customer must still return to the service center for the pre-determined appointment date between 77 and 90 days for the calibration.

Non Software Requirements

Training

Manufacturers will be required to train their own employees using the electronic reporting system.

Documentation

The Department will issue each manufacturer a certificate letter upon completion of 3 successful electronic reporting tests.

Certified Ignition Interlock Device Summarized Reporting Record Layout.

POSITION	LENGTH	LEVEL	*-----FIELD NAME-----*	FORMAT
00001	00474	01	INREC	GROUP
00001	00003	03	MANUFACTURER_ID	C 3
00004	00003	03	PROVIDER_ID	C 3
00007	00003	03	INSTALLER_ID	C 3
00010	00030	03	LAST_NAME	C 30
00040	00030	03	FIRST_NAME	C 30
00070	00030	03	MIDDLE_NAME	C 30
00100	00008	03	DOB	C 8
00108	00025	03	DL_NUMBER	C 25
00133	00008	03	INSTALL_DATE	C 8
00141	00008	03	MVD_UNINSTALL_DATE	C 8
00149	00008	03	REMOVAL_DATE	C 8
00157	00001	03	REPORT_TYPE	C 1
00158	00001	03	NON_COMPLIANCE_CODE	C 1
00159	00004	03	BAC_VIOLATIONS_COUNT	C 4
00163	00002	03	RETURNED_ERROR_CODE	C 2
00165	00008	03	DEVICE_DOWNLOAD_DATE	C 8
00173	00011	03	DEVICE_DOWNLOAD_TIME	C 11
00184	00008	03	TAMP_CIRC_DATE	C 8
00192	00008	03	BAC_VIOLATION_DATE1	C 8
00200	00008	03	BAC_VIOLATION_DATE2	C 8
00208	00008	03	BAC_VIOLATION_DATE3	C 8
00216	00018	03	DEVICE_ID	C 18
00234	00012	03	TECH_ID	C 12
00246	00001	03	BYPASS_APPROVAL	C 1
00247	00011	03	BYPASS_TIME	C 11
00258	00006	03	VIN	C 6

00264	00003	03	INTERLOCK_ORDER	C	3
00267	00011	03	BAC_VIOLATIONS_TIME1	C	11
00278	00003	03	BAC_VIOLATIONS_VAL1	C	3
00281	00011	03	BAC_VIOLATIONS_TIME2	C	11
00292	00003	03	BAC_VIOLATIONS_VAL2	C	3
00295	00011	03	BAC_VIOLATIONS_TIME3	C	11
00306	00003	03	BAC_VIOLATIONS_VAL3	C	3
00309	00002	03	TAM_CNT	C	2
00311	00011	03	TAM_TIME1	C	11
00322	00011	03	TAM_TIME2	C	11
00333	00002	03	CIR_CNT	C	2
00335	00011	03	CIR_TIME1	C	11
00346	00011	03	CIR_TIME2	C	11
00357	00002	03	ROLLNG_RTEST_VIOL_CNT	C	2
00359	00011	03	ROLLNG_RTEST_TIME1	C	11
00370	00011	03	ROLLNG_RTEST_TIME2	C	11
00381	00011	03	ROLLNG_RTEST_TIME3	C	11
00392	00011	03	ROLLNG_RTEST_TIME4	C	11
00403	00011	03	ROLLNG_RTEST_TIME5	C	11
00414	00011	03	ROLLNG_RTEST_TIME6	C	11
00425	00050	03	SEND_AS_RECEIVED	C	50

***** Bottom of data *****

All Dates are in YYYYMMDD format

All times are in HH:MM:SS:HS