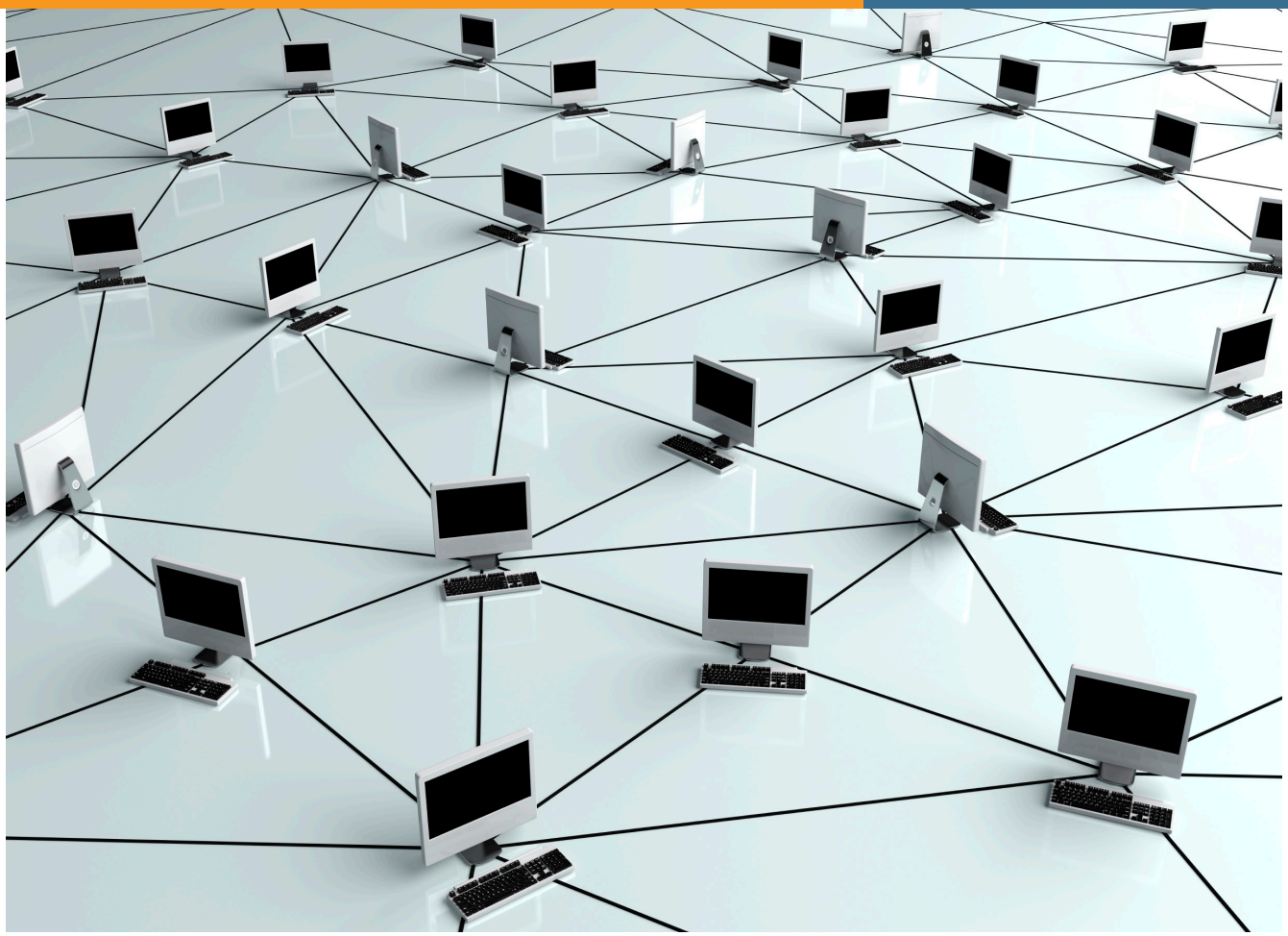
TRAFFIC INJURY RESEARCH FOUNDATION



ALCOHOL INTERLOCK PROGRAMS:
DATA MANAGEMENT SYSTEM IMPLEMENTATION

TIRF

The knowledge source for safe driving

The Traffic Injury Research Foundation

The mission of the Traffic Injury Research Foundation (TIRF) is to reduce traffic-related deaths and injuries. TIRF is a national, independent, charitable road safety institute. Since its inception in 1964, TIRF has become internationally recognized for its accomplishments in a wide range of subject areas related to identifying the causes of road crashes and developing programs and policies to address them effectively.

This report was produced with financial assistance from the National Highway Traffic Safety Administration (NHTSA).

Authors

Robyn D. Robertson
Erin A. Holmes
Ward G.M. Vanlaar

Traffic Injury Research Foundation
171 Nepean Street, Suite 200
Ottawa, Ontario K2P 0B4
Ph: (613) 238-5235
Fax: (613) 238-5292
Email: tirf@tirf.ca
Website: www.tirf.ca

Traffic Injury Research Foundation

ISBN: 978-1-926857-43-5

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

TIRF gratefully acknowledges the assistance of the following individuals who shared their knowledge of alcohol interlock initiatives and vendor oversight during the development of this report in 2010 and who reviewed and commented on earlier drafts. Their insights, experiences, and expertise allowed us to create a user-friendly, practical report that can benefit practitioners across the country.

Brett Close
Operations Manager
Driver Control Customer Service
Colorado Department of Revenue

Leighton Isles
Director
Tarrant County Community Supervision and Corrections Department

Susan McKinney
Administrator, BAIID Division
Illinois Secretary of State

Tom Roy
Commissioner of Corrections
Minnesota Department of Corrections

Will Speaks
Senior Architect
South Carolina Dept. of Probation, Parole, and Pardon Services

Toby Taylor
Ignition Interlock Program Administrator
Oklahoma Board of Tests for Alcohol and Drug Influence

Mike Balgord
President
National Interlock Systems, Inc.

Jim Ballard
President & COO
Smart Start Inc.

Debra Coffey
Vice President, Government Affairs
Smart Start Inc.

Felix Comeau
President & CEO
Alcohol Countermeasure Systems Corp.

Scott Elting
Interlock Product Manager
Draeger Safety Diagnostics, Inc.

Luz Mitera
Application Support Services Manager
Alcohol Countermeasure Systems Corp.

Denise Connerty
Business Unit Manager, Compliance Monitoring
Alcohol Countermeasure Systems Corp.

INTRODUCTION

An automated alcohol ignition interlock program reporting system serves to automate routine tasks relating to the management of interlocked offenders. Jurisdictions can benefit from such an automated system, particularly if a potentially large number of offenders are expected to participate in the interlock program now or in the future. For example, a jurisdiction may consider developing an automated system if first offender legislation is passed and program participation numbers are expected to increase as was the case in Illinois. Failure to automate and continued reliance on paper-based reporting systems can lead to offenders slipping through gaps in the system or being overlooked as a result of lack of staff, weak communication channels, and untimely exchange of information between various agencies.

Benefits of automation

While there are considerable cost implications up front, there are also multiple benefits and great value in the development and implementation of an automated data management system. Through automation, agencies can:

- Streamline program activities;
- Reduce or provide for the re-allocation of existing staff and workload;
- Improve program management;
- Improve data integrity and security;
- Increase the timeliness of updates and the exchange of information;
- Increase efficiency of communication and messaging from the administering agency to offenders and service providers;
- Increase control and management of any existing financial assistance program for offenders; and,
- Facilitate program evaluation in the long-term.

The implementation of an automated data management system has the potential to make offender management much more efficient and save jurisdictions money by increasing efficiency and decreasing staff workload. To use Maryland as an example, the Motor Vehicle Administration (MVA) pioneered an automated interlock monitoring program that combines electronic data receipt and program management which led to a reduction of an average of 20,000 paper documents each month.

Other states such as Colorado, Illinois, Florida, New Mexico, and South Carolina also have good examples of automated data management systems that can provide guidance to jurisdictions that are planning for or working towards automation.

Paper-based reporting

For those jurisdictions that are not able to move forward with the implementation of an automated data management system at this time, an interim plan can help to manage the influx of data which comes with interlock program growth and/or expansion. The development of protocols to collect and manage interlock data are needed in conjunction with a manual means to complete tasks (i.e., human interaction as opposed to electronic exchange) until an automated data management system is feasible. However, jurisdictions cannot overlook that with any paper-based reporting system, agencies run the risk of offenders avoiding program participation or monitoring, often as a result of workload, processing delays, and untimely

exchange of information between different interlock program partners in the short-term. Reliance on a paper-based reporting system serves to increase staff and workload, increase the potential for errors or omissions, and can impede offender monitoring and agency communication.

At present, most U.S. jurisdictions still have paper-based reporting systems in place. This is likely to change as many of these programs continue to grow and evolve. Growing recognition of the value of, and potential savings from having an automated system in place can be the impetus for more jurisdictions to make the transition from paper-based systems in an effort to improve the quality and efficiency of monitoring and services. Although the development of an automated reporting system brings with it significant costs, it can improve the delivery of the interlock program and enhance offender tracking. More importantly, the automation of data management can result in savings in the long-term.

Methodology

In December 2010, a two-day workshop was organized in Toronto to bring together program administrators and vendors to discuss the issues of vendor oversight and automated data management systems. Representatives from four interlock vendors (ACS, Draeger, Lifesafer, and Smart Start) were in attendance along with program administrators from Colorado, Illinois, Minnesota, Oklahoma, Texas, and South Carolina. The focus of discussions included state and vendor experiences with data management and reporting, core steps to develop a data management system, and essential elements of a data management system. This report, along with a companion piece entitled Alcohol Interlock Programs: Vendor Oversight (released in 2011) was borne out of those discussions.

Contents of report

This document provides an overview of some important issues to consider when transitioning from a paper-based system to an automated system. It is structured in four key sections:

1. Plan development;
2. System components;
3. Essential system requirements;
4. Vendor interactions.

An automated data management system implementation checklist for agencies is also included in Appendix C.

While this information is essential to anybody involved in designing an automated solution for the management of an interlock program, it warrants mentioning that this document is not meant to serve as a step-by-step manual for the actual development of such an automated system. Such a manual requires the involvement of a software development team that adopts a structured approach tailored to the specific needs of developing specialized business solutions. Rather, this document is meant to provide broad guidelines as well as some specific details with respect to alcohol ignition interlock programs that are particularly relevant in preparation of, and during, the development and delivery of an automated data management system. The information in this document is based on the experiences of program administrators and device manufacturers.

PLAN DEVELOPMENT

Ideally, consideration should be given to the creation of an automated system as part of the planning and implementation phase of an interlock program. However, many interlock programs were first designed and implemented during a time when automation of processes was not easily achieved and/or when automation was not necessarily deemed useful, for example because the number of participants in the program was small. As a result, automation is often considered after a program has been established for several years and at a time when offender participation has grown sufficiently to warrant such a step.

Regardless of when the issue of automation is raised, the development of a plan to streamline the transition from a paper-based to an automated system is a necessary first step. This plan describes what priority pieces of information should be collected, how that data can be collected, who will collect the data, where the data will reside, who will own the data, and with whom the data must be shared. Examples of sources of data to consider include:

- data collected by the interlock device;
- information about participants using the device;
- information about program operations; and,
- information about program components (e.g., sanctions or reinforcements that are applied).

The information that is collected may not only be relevant to the management of the interlock program itself, but also to any future evaluation.

Essentially, the plan development phase involves an "environmental scan" of the existing data system/practices (i.e., either manual or automated) and the context within which the interlock program operates; both information pertaining to the jurisdiction's own program as well as information about data management systems in other jurisdictions should be collected and reviewed as part of a scan. This activity is useful to inform the development of business process flowcharts that illustrate in much detail how the program functions, which stakeholders are involved, what responsibilities they each have, how and when they are supposed to communicate, and how and when the exchange of information takes place. Information from other jurisdictions is important to help identify gaps in the existing program, opportunities for improvement, and how this has been achieved in other places. The following tasks are important components of this environmental scan:

- **Review existing interlock data system (manual or electronic).** Review any existing interlock data system to collate and manage reports from interlock vendors regarding different classes of offenders (including new ones) and to generate automatic responses to a range of events. Make a draft list of all of the actions that will be required of the interlock data system with regard to offenders.
- **Assess existing driver records system.** Conduct an assessment to determine whether updates are needed to the existing driver records system in order for it to interface with the interlock program system and determine if there are resources available to make these improvements.

  Update the existing driver records system to accommodate any new classes of interlock offenders (e.g., first offenders). To clarify needed changes, it is helpful to create a draft list of all of the actions that are expected to be performed by the automated system.
- **Review linkages.** Review linkages between the driver records and the interlock data system to accommodate any new classes of offenders.

- **Estimate costs and budget.** Gather estimates of the costs associated with the creation of an automated system at the outset as they can be quite high. Also, costs to run the system and ongoing maintenance costs should be considered at this stage. Determine whether sufficient funds are available to develop an automated system.

- **Designate a lead person.** Designate a DMV[1] (or other involved agency) staff person who is knowledgeable in database design and management and/or automation to be actively involved in the development process and assign this person to manage contractors hired to build the automated system (e.g., to act as an application development project manager). Agencies should not count on an outside contractor to understand the many facets of the program in conjunction with current capabilities and future needs. A person representing the agency authority who possesses a good understanding of the scope of the project and current processes and who is able to anticipate future enhancements is essential to the successful completion of these tasks.

- **Discuss governance.** Discuss governance policies related to data ownership, access, and sharing. This aspect of the task will present challenges that must be carefully negotiated, and will take time to resolve. Almost all agencies are rightfully protective of their data and may be resistant to provide access to others. Agencies may also be subject to specific policies that prohibit the release of data. These issues can be overcome but it is likely that concessions will be part of the process.

- **Meet with partners.** Investigate the structure and accessibility of court and correctional data systems to facilitate the sharing of information across systems and communication among agencies as appropriate. Law enforcement and treatment data systems should be similarly explored in this regard. At a minimum, if court professionals are involved in the interlock initiative, it will be important that agencies are able to share offender status and conviction information to identify eligible offenders and track progress.

  Meet with interlock vendors early on and request that they be involved in concept development. As part of this task, it is important to explore whether each vendor's respective data management system is able to interface with any new system utilized by the agency authority. These interfaces can be costly so planning is indispensable to minimize unanticipated costs downstream. In this regard, it can be useful to consider the interface systems developed in other jurisdictions (e.g., Colorado and South Carolina) as a template to work from in order to manage costs associated with this task.

- **Reach consensus.** It is essential that agencies agree upon the information that will be included in the system and shared across agencies and localities. Moreover, the importance of well-defined criteria that are clearly articulated to vendors regarding what pieces of data they are required to capture and report is paramount. As part of this task consider the following:

  - What data are agencies expected to report?
  - Who is the data reported to?
  - Who is filtering the data?
  - Who has access to the data?
  - How much information will be made public and how much will be protected against disclosure and how will it be protected?

As part of the development process, jurisdictions are encouraged to also take into account the following considerations:

[1] DMV (Department of Motor Vehicles) refers to the state licensing agency; the name of this agency may vary from one jurisdiction to the next, but each has a licensing agency.

- **Standardized reporting procedures.** This is important so that paperwork from different agencies shares a common format and information regarding specific offenders can be uniformly updated. This enables relevant agencies to track progress in relation to specific cases.
    - While standardized reporting is important, it is also necessary to have ad-hoc capabilities. It is difficult to know whether standardized reports created during the early development stages of the automation process will be sufficient or what information requests will be received from outside agencies in the future. There must be flexibility to ensure that accommodations can be made if changes occur downstream.
- **Timelines.** Do not underestimate the time required to develop and implement an automated data management system. This task can be challenging and time-consuming. Delays should be expected and proposed timelines should be sufficiently flexible to accommodate this. It is beneficial to get time estimates from an experienced staff member, contractor, or both, and to review these timelines regularly.
- **Privacy.** Acknowledge that privacy, civil liberty, and confidentiality issues influence decision-making related to this task. In response to growing government mandates and requirements that personal information be protected, these issues will likely increasingly influence information-sharing protocols and permissions.
- **Reciprocity.** Reach out to neighboring jurisdictions to discuss reciprocity for alcohol interlock programs and to ensure that those offenders that cross jurisdictions are not able to avoid the use of the device. This may be particularly applicable to smaller jurisdictions with multiple borders and those that experience the movement of offenders across jurisdictions for the purposes of employment and leisure activities. Facilitating the sharing of information between different agency authorities, as well as jurisdictions as appropriate, can be beneficial.
- **Compatibility.** Account for technological differences across agencies (e.g., courts, DMV) within a jurisdiction as some may not have the same capabilities as others.

  Confirm that what is built as an interface will work with vendors and investigate what has been built in other jurisdictions that can be used/borrowed/modified to reduce costs. This can also reduce implementation time because the front-end development is largely completed (cf. South Carolina's software framework that is freely available to jurisdictions across the U.S. – see Appendix B).

  Those jurisdictions that contain or are connected to Tribal lands may involve additional consideration with regard to the development of a data management system for the interlock initiative. Due to the fact that tribal governments are sovereign, jurisdictions can negotiate data-sharing agreements with them to the benefit of both jurisdictions (see for example New Mexico).

Taking into account all of these tasks and considerations, the core steps to develop an automated data management system include:

- Create a workgroup and assign leadership and other roles to ensure accountability and transparency, and to streamline the process.
- Schedule an internal meeting of stakeholders to identify current practices and existing gaps.
- Translate the current data system (manual or automated) into business rules and workflow. This step is the foundation for a uniform understanding of activities, responsibilities, and processes across stakeholders.
- Review what other jurisdictions are doing (i.e., what is working well elsewhere).
- Develop a clear understanding of what the ideal system would look like (i.e., the combination of

the existing system with improvements based on identified needs and strategies that work well elsewhere).

- Incorporate the ideal system into business rules and workflow.
- Determine the following:
  - Who would data be collected from?
  - What agencies would need access to the system and at what level?
  - How would data be shared?
  - What confidentiality/security issues have to be considered?
  - What are the costs of different pieces of the system?
  - What is the achievable scope of the work (i.e., will the entire automation process take place in-house or will it be subcontracted)?
- If a subcontractor is required to design the automated system, issue an RFP[2] to hire a software developer.
- Develop quality assurance protocols and testing protocols to ensure the delivered solution will work well for all stakeholders.

[2] States define differently what an RFP is in their procurement system. Typically it is used when an agency knows what they want done, but not how it should be done. For example, an RFP might apply to a state implementing a new interlock program when they are unaware of how interlocks work, what the industry standards are, and so forth. If an agency intends to support custom software development, they should also have the skills to do so – as such, an RFP may not be a good fit.

SYSTEM COMPONENTS

Generally speaking, an interlock data management system consists of a central repository that integrates several data components including:

- agency requirements;
- business management;
- the interlock device; and,
- service centers.

A brief explanation of each component is provided below.

- **Agency requirements.** These requirements are defined by the state agency that oversees the interlock program. Examples of these requirements can include:
  - Data files: format and security protocols (e.g., how are data to be structured and sent?).
  - Reports: rules regarding reports for failure to appear, violations, removals, compliance, installations, and so forth.
  - Web access: security protocols for access to client data, event data, summary reports, service history/next appointment, violation data.
  - Notifications: flags such as failure to appear, violations, removals, compliance, installations, and so forth.
- **Business management.** Examples include pricing control, service center productivity, and service center workload.
- **Interlock device.** The device captures and stores data however, these data can vary across manufacturers. Typically devices are programmable and can accommodate a range of different program requirements (e.g., pre-set level, emergency override, running retests). A database should be maintained in which the data from all interlocks are captured and retained. At a minimum, the database should be capable of capturing and reporting information such as ignition attempts, starts and stops, BAC levels, refusals, and circumvention attempts along with the date and time of each of these events.
- **Service center.** At the service center client data download from the device and data entry occur (e.g., monitoring schemes can be uploaded). Business practices at service centers include client scheduling, client contracts, revenue reporting, and invoicing.

To facilitate communication across these different components, the data management system must have interface capabilities. For example, the interlock vendor's system must be able to communicate with the driver records system that is managed by the state. If an interlock program also has a judicial or correctional component, interfacing with these systems is another consideration. The system also requires reporting capabilities where information from the service center is transmitted to case managers in a timely fashion. Lastly, if the interlock program has indigency or unaffordability provisions, there is the potential for linking opportunities to driver tax records or other forms of assistance such as food stamps or eligibility for other financial assistance programs (see New Mexico[3]). At a minimum, the number of offenders who are not able

[3] For example, in New Mexico offenders are required to show proof of participation in one or more of the following types of public assistance programs: Temporary Assistance of Needy Families (TAN F), General Assistance (GA), Supplemental Nutritional Food Assistance Program (SNAP), Supplemental Security Income (SSI), or Food Distribution Program on Indian Reservations (FDPIR).

to afford to participate in the interlock program should be tracked in order to gauge the magnitude of the issue.

Additional considerations include:

- A system must be able to sufficiently interface between driver records (DMV) and vendor systems to facilitate the sharing of information, and potentially facilitate communication, in relation to a number of issues. For example, if issues are noted (e.g., invalid driver's license number) technicians can inform the offender to contact the program administrator to address the matter at the time of installation which can facilitate resolution more quickly and ensure that offenders get the interlock installed and participates in the program as opposed to driving unlicensed. Also, the automatic population of forms ensures accuracy and reduces the likelihood that technicians will make unnecessary errors entering information.
- Vendors are required to comply with all reporting requirements outlined in law or mandated by the jurisdiction. From a business management perspective, vendors may also be required to submit quarterly reports to the state that confirm that data are downloaded from interlocks in a timely manner, that they have evaluated the data, and that it has been made available to the state within the required timelines. Vendors may also be required to certify that all data are accurate and agree to submit reports when requested for use as evidence with court or administrative hearings.
    - Examples of business management reports that can be submitted to the agency that oversees the interlock program include fail reports, de-installation reports, and reports that identify drivers who have failed to return for a data download.
    - Vendors may submit a nightly report and letters can be printed based on the violations recorded. Extensions and cancellations of interlock licenses can be done automatically based on the information submitted by the service provider to the DMV.
- The system should be able to interface with multiple agencies to provide and receive information. Interaction should occur for every installation, removal, change in vehicle, and monitoring.
- Involve the judiciary in the process as appropriate; it is essential to ensure that court case information is shared with driver records. A system should have judicial and administrative elements to ensure that all relevant data are collected and kept in a centralized location.
- If the offender is on probation, create linkages with their case management systems in order to track offender compliance and share information.
- It is possible to interface with tax records for the purpose of determining whether offenders cannot afford the interlock. This can automatically determine whether or not a person would qualify for funding. A process like this exists in Colorado where their system has a reporting relationship with the Department of Revenue tax branch.

  As part of this process, also consider developing means for tracking the number of offenders deemed unable to afford the interlock to gain a better grasp of the magnitude of the problem. This can facilitate the management and allocation of funds based on need and/or demand.

ESSENTIAL SYSTEM REQUIREMENTS

The development of standardized violation definitions and violation reports are essential to any successful interlock program. This is true regardless of whether the program is automated or not. However, automation requires standardization; or, in the absence of any standardization efforts, benefits that can accrue through automation are limited.

Standardization is needed to create consistency in offender management and eliminate confusion among stakeholders within a jurisdiction. By capitalizing on such consistency, automation can reach its full potential and lead to increased efficiency. Administrators and vendors also agree that there is a need for the standardization of terms at least within agencies in a single state to promote consistent delivery of the interlock program (e.g., What is a violation?; What events can occur?).

Standardized violations. Prior to the implementation of a data management system, violations must be clearly defined at the state level. The definition should be fairly restrictive as it is not favourable to have a loose definition that is open to interpretation, as this can, and has, led to different practices across vendors. This is not only problematic from the point of view of equality of the law but, as mentioned above, it will likely also make the automation process more challenging, if not impossible. To facilitate this process, a data dictionary containing a clear description of all events and violations should be drafted. The Association of Ignition Interlock Program Administrators (AIIPA)[4] has begun to look at this issue and endeavors to create a set of standardized violation definitions.

Common violations that are agreed upon by most vendors include:

- Failed breath tests;
  - BAC readings and patterns of BAC readings (state to define level)
- Missed/failed running retests;
- Aborted start attempts;
- Bypass/circumvention/tampering attempts;
  - Power disconnections
- Engine starts and stops;
- Handset disconnections and/or device removals;
- State requirement that there be a follow-up breath test after some events;
- Emergency override;
- Violation resets and early recalls;
- Camera obstruction; and,
- General catch-all for previously unidentified violations (e.g., not using device as required – see for example Illinois).

[4] AIIPA is an organization composed primarily of state, county, parish, or municipal employees who provide specialized knowledge to an ignition interlock program. AIIPA promotes best practices, enhancement of program management, and the provision of technical assistance to improve traffic safety by reducing impaired driving. For more information, please visit: www.aiipa.org.

While clear and standardized violation definitions are necessary, program administrators should be afforded some flexibility in how they address violations. It is important to be able to take the context of violations (i.e., the events directly preceding and following the alleged violation) into consideration. Currently, some states do not permit the examination of context. However, it is preferable to take such contextual information into account in order to address issues such as false positives. If permitted by law, a process is needed to guide the review of such contextual information. To best manage this process, definitions should be determined by the state authority in administrative rules and not written in legislation to allow for reasonable flexibility in decision-making. Program administrators have found that when such rules are written in legislation they often tend to be too rigid, leaving no flexibility to adapt or adjust them, for example when new situations arise that cannot be addressed within existing parameters. This often has the unintended negative consequence of prematurely removing offenders from the program.

In addition, criteria are required to standardize how decisions are made to disregard a noted violation that turns out to be a false positive. This responsibility can be delegated to either the monitoring agency or the vendor.

Standardized reports. Standardized reports are critical in terms of efficiency. From a technical point of view, the submission of vendor reports is a digital transfer from one system to submit data to another. It is important that the format of this data transfer is standardized. If all vendors are required to submit standardized reports, this can reduce or eliminate discrepancies across vendors (for a list of important standardized reporting form considerations, please refer to Appendix D). Another important issue to resolve prior to implementation relates to where and when violation reports are to be sent and who is allowed to have access to or review them.

For examples of reporting samples from Illinois, Maryland and New York, please refer to Appendix A.

To this end, vendors have the capabilities to report both in real-time or overnight using batch reporting. Real-time reporting of violations can assist in ensuring swift and certain sanctioning in both court and administrative interlock programs and automation can reduce this processing time. However, this may require 24-hour staffing of the system to ensure swift responses, which can become resource intensive. To avoid this, a system could be fully automated meaning that both input and output are automated and thus, does not require the staffing of a station. The state should consider which type of reporting best suits their need without unduly depleting available resources or funding.

Agencies must rely on servers to operate 24/7 to keep the system operational. Given that servers are separate from software, both server and network employees need to be included in system upgrade discussions so that they are aware of any up-time[5] requirements. Servers also go down on occasion and, as a result, there must be some form of contingency should the server be rendered non-operational.

Another important consideration related to reporting is whether the filtering of data (i.e., the process of summarizing all the raw data into a limited number of reports regarding confirmed events) will be undertaken by the monitoring agency or the vendor at the national level. There are pros and cons associated with each of these options that should be weighed by the monitoring agency. A minimum set of recommended filters for data should be developed (more information on filters is contained in the 'Vendor Interactions' section). The state should also not rely on service centers, technicians, and subjective reporting only; instead, there should be vendor management so that reporting is objective, transparent and consistent.

[5] Up-time requirements generally refers to the total amount of time that the system is available for end-use applications. The value is stated as a percent of total scheduled working hours.

Communication. Efficient strategies to communicate across all of the agencies involved in program delivery are essential to the success of the interlock program. It is important to recognize that the complexity of communication will increase with the number of agencies that report/receive information from the system. As a result, issues and delays can arise and should be anticipated during the implementation phase (see South Carolina for an example of system communication among multiple agencies). As such, it is important to identify and resolve as many of these issues as possible early on during implementation so that they do not go unaddressed and create bigger problems downstream.

One such issue that frequently arises relates to the receipt of messages. Messages must be well defined and the receipt of messages must be confirmed to ensure follow-through and facilitate accountability. Another example involves noting the correctional status of offenders in their interlock files (i.e., whether they are on probation or involved in the correctional system) so that agencies know to communicate with probation officers to share information about offender compliance and relevant activities.

Other important aspects of communication to consider include:

- Messages must be well defined: This means it has to be clear what data an agency wants to receive and send. Agreements that list data needs for each stakeholder are essential.
- Messages must be guaranteed: This means the receiving systems must acknowledge receipt of messages and a protocol is necessary to handle non-confirmed messages.
- Error messages must be reduced: This means that there must be a system in place to address and resolve error messages as they occur in a timely and accurate fashion. If messages are both well-defined and guaranteed, the number of error messages that occur can be minimized. This can result in less staff and/or resources that are needed to review them.

Similarly, if an offender is found to have violated the interlock program rules, they must be notified of their non-compliance. Decisions have to be made about how this notification will occur. Most often, offenders receive a letter that advises them that they were non-compliant during the previous reporting period. These letters can be automatically generated (see for example the process used in Illinois). Another option is to also notify offenders that they have been compliant using the same process. The rationale behind notifying offenders of both non-compliance and compliance is that it holds them accountable for negative behavior (violations) and reinforces good behavior (lack of violations).

Security. Automated data management systems open agency servers to the internet to allow vendors to submit data electronically. This creates significant security concerns that can be greatly minimized if servers operate on either private networks or secure state networks. By necessity, the communication between vendors and state agencies includes personal and/or sensitive information. It is important to guarantee that this information cannot be accessed or altered by a third party. If a third party were to submit fraudulent data, it could result in embarrassing communications from the state agency or incorrect violation penalties. Issues of privacy protection and liability are also of concern. For these reasons, it is of the utmost importance that all data submissions are authorized and communication is securely encrypted to protect the integrity of the interlock program. Policies regarding the transmission of data and communication between vendors and agencies should be created to address some of these security concerns. When creating these protocols, error codes should be defined and contingency strategies for addressing these error codes should be created.

As an example, the Road Traffic Authority for the Netherlands (RDW) has examined the issue of personal data protection extensively as a component of interlock program implementation. In the Netherlands, the integrity and confidentiality of interlock data must be ensured. As a result, the Privacy Act and Dutch Protection Authority supervise the collection and storage of data to guarantee that it is not misused or

manipulated. For this reason, the installer and/or vendor is not allowed to see the interlock data and it is stored in one central register that is owned by the government. Only vendors and installers who meet the requirements regarding data processing and transfer may supply interlocks for the Dutch program.

Other important requirements that are considered essential to an automated data management system for interlock programs include:

Functionality of system. Any automated system must have the ability to perform a variety of tasks and consist of multiple components. Functionality that every interlock system should consider includes:

- A combination of exact and probability matching protocols to increase the likelihood of successfully matching records from offenders coming from different sources ;
- Automatic generation of forms and notices;
- Multiple user profiles and different levels of access;
- Linkages across files (to accommodate for any updates);
- Web-based applications;
- Accessible records of participant history in the interlock program (by extension this could include criminal history outside of program participation);
- A data back-up and disaster recovery plan (e.g., what happens if the server or internet connectivity is down?);
- The ability to account for different time zones; and,
- The ability to upgrade and include build-outs and add-ons (such flexibility is needed to adapt to new needs).

Distinguish between multiple interlock offender groups. It is important to distinguish between various offender groups such as first and repeat offenders because they may have different program rules apply to them. For example, repeat offenders could have more stringent requirements. Vendors must be aware of an offender's status and of the program rules that apply to them at the time of installation so they can properly instruct each offender.

Involvement of other agencies. If other agencies are involved in the interlock program in a peripheral capacity (e.g., probation or treatment), they may still need to be included in the implementation process. Channels of communication have to be established and determinations need to be made as to their level of access to interlock data.

Comment field. Vendors as well as interlock case managers should have the ability to include comments in an offender's file in order to note progress/compliance issues or other relevant information.

Indigency and/or affordability indicators. If a vendor is responsible for making affordability determinations or if they are instructed to provide a reduced rate for an offender, indicators must be established.

VENDOR INTERACTIONS

Based on experiences in several jurisdictions, it has been recognized that vendors are a constructive and integral partner in the development and delivery of a data management system. While their participation may require some management, it is essential to take into consideration the wide range of interactions with and differing capabilities of vendors and involve them early on in the development process. Generally speaking, any stakeholder that will be expected to use the system should be included in its development, and this is also true of vendors. In order for vendors to assist in the development of the automated system, they must be provided with clearly defined goals. Questions that can be addressed with vendors include:

- What data will be collected?
- Who will have access to the data?
- How will data be received and processed?
- Who will filter the data?
- What actions will be taken as a result of the data collected?
- Where is the data going to be stored?
- Who will have ownership of the data?

Expectations of vendors with regard to data management should be clearly defined within contracts or requests for certification to ensure transparency and accountability. Ongoing communication during the development, implementation, and delivery of an automated system can also facilitate this transparency and accountability. Therefore, agencies should consider the following:

- There must be good communication between vendors, the DMV, and other agencies involved in the delivery of the interlock program. Vendors require feedback on the information that is submitted (e.g., if a date of birth does not match, real-time reporting can allow the DMV to explain the mismatch while the offender is at the service center to have an interlock installed).
- Agencies need to let vendors know the size of files that they are capable of handling and define the number of records or pieces of information that are to be sent.
- Training is necessary for those who review data and make determinations as states need to know what the data mean. This training can be provided by vendors as appropriate.
- An updated list of installation sites must be maintained by the monitoring agency.
- Service providers are often unaware of which offenders are court-ordered to install an interlock. Such a lack of follow-up is often a major issue so improved communication with courts, probation, and service providers can help overcome this.

The filtering of data is also an important part of the data management process. Filtering is a necessary step to summarize the raw data into meaningful packets of information. It reduces the data into reports containing only the information that is relevant in light of the program rules, for example reports about program violations. The program administrator can filter the data or vendors can manage this task. On a positive note, vendor filtering and reporting of data means less training and interpretation for the monitoring agency. This can be beneficial especially if staff turnover is high. On the other hand, some monitoring agencies choose to filter the data themselves as a way to gain more control over the program.

Regardless of which option is chosen, it is essential that some ground rules about filtering data are established to increase consistency and transparency across the program. For example, if vendors are responsible for filtering data, auditing procedures need to be put in place. Vendors often have these procedures in place already and typically consist of reviewing a selection of data logs for quality assurance purposes. A state agency can conduct an audit of a random selection of files as part of its vendor oversight protocol to ensure that reporting meets the requirements outlined by the state.

CONCLUSIONS

The development and implementation of an automated data management system for interlock programs can be a complex and resource-intensive task. However, automation can greatly improve the efficiency and effectiveness of an interlock program in tracking offenders and monitoring their compliance which will become increasingly important as programs grow and expand. To this end, an automated system reduces opportunities for error, ensures that relevant data are consistently captured, improves communication, and supports future evaluation efforts.

Not only can an automated data management system facilitate a more seamless approach to program delivery and the processing of participants, but it has the potential to accrue cost-savings from an operational perspective. As such, the expectation is that automation efforts will lead to a return on investment. Each jurisdiction should plan carefully when considering the transition to a fully automated system. Each system will be different but common features can be borrowed from other jurisdictions to make the process less onerous. Consultation with stakeholders and the involvement of vendors in the planning and implementation phases are of paramount importance. For step-by-step considerations in the implementation process, refer to the checklist in Appendix C.

APPENDIX A – REPORTING SAMPLES

The following are examples of reporting samples from various jurisdictions. These materials illustrate some of the different pieces of information that monitoring agencies require to be reported to them by vendors. Each jurisdiction has different requirements which are typically outlined in administrative rules. Standardized violation definitions and clear requirements as to what should be reported make the reporting process easier and more efficient for all parties involved in the delivery of the interlock program.

Materials from the following jurisdictions, Illinois, Maryland, and New York are included.

ILLINOIS

The following information is provided to new vendors in Illinois for the exporting and layout of device data reports.

Input text file layout for BAIID

The file is to be a text file with all fields in each record being delimited by a semi-colon (;). All fields are required unless otherwise specified.

Header record (Should be one header record per driver being reported.)

Name:	**Size:**
Description	**Notes**

Record type 1 char Header indicator Constant value "H"
DL Number 12 char Drivers License number format Annnnnnnnnnn
Company ID
Start Date
End Date

separated by '; '(semicolon) Drivers license #, Name of individual, Company ID, various start to end dates.

Detail Record

May be one to many detail records as necessary to report all activity for the BAIID Device. Activity is the event, test, or action recorded by the BAIID. All fields may be variable length although many will fill the size specified. ALL values separated by semicolon

NAME:	SIZE:	DESC:	FORMAT:
Record type	1 char	Header indicator	Constant value "D"
DL Number	12 char	Drivers License number	format Annnnnnnnnnn
DAY	3 char	day of week	Sample values "MON", "THU"
DATE	8 char	date of activity	mm/dd/yy
TIME	5 char	time of activity	hh:mm
Activity	15 char	(tests, retest etc)	text, free form punctuation, see note 1
BAC level	4 char	BAC Reading	.nnn note decimal position.
Result	20 char	Device action/result	text, See Note 2 and Note 3

Note 1
Sample values for Activity are "engineON", "Car Not Started", "TestTaken", "EngineOFF", "RandomTest" , "USER ABORT", "*POWER OFF", "*POWER ON"

Note 2
Sample values for Result "PASS", "FAIL" , "Invalid sample --- pressure","Rolling retest - Toot horn", "Breath samples requested: 5","Rolling retest - Blast horn", "BYPASSED", "REFUSED"

Note 3: The preferred format for tests are “PASS”, “FAIL” or “ “ (spaces, equates to pass) passed, failed are acceptable.

Violations

violation code 04 Failure to complete rolling retest
for each violation
7th field indicates “retest refus”

violation code 05 High BAC
for each violation
Data file 7th filed indicates “fail”
And has BAC level => .05

Violation code 07 Tamper
for each violation
7th field indicates “bypass” or “Tamper”

violation code 02 5 or more unsuccessful attempts to start (24 hrs)
for each day
b.bac >= .025 and result = 'FAIL' count > 4
and it is NOT a retest
group by day (24 hour period)

Data criteria: BAC reading of >= .025 is a FAIL

violation code 06 10 or more unsuccessful attempts to start reporting period
b.bac >= .025 and result = 'FAIL' count > 4
and it is NOT a retest

Low BAC pattern violation code 02
current program checks for 4 or more .025 within the reporting period (60 days)
This is higher level then 5 or more in 24hrs, and 10 or more in period

Other Violations not handled by this program
Violation 01 Calibration not completed (no monitor report received) for reporting period.
Violation 09 Failure to install BAAID in allotted time period.

MARYLAND

Data sample received from the data logger of a ignition interlock device.

Date	Code	Description	BAC
02-10-2013 11:12.00 am	3002	Pass	0
02-10-2013 11:20.00 am	3009	Retest req	
02-10-2013 11:21.00 am	3002	Pass	0
02-10-2013 01:18.00 pm	3000	Handset power	
02-10-2013 01:19.00 pm	3001	Power on	
02-10-2013 01:21.00 pm	3002	Pass	0
02-10-2013 01:21.00 pm	3005	Car run	
02-10-2013 01:30.00 pm	3006	Car stop	
02-10-2013 01:40.00 pm	3001	Power on	
02-10-2013 01:41.00 pm	3015	Fail	.038
02-10-2013 01:47.00 pm	3005	Car run	
02-10-2013 01:47.00 pm	3002	Pass	.004
02-10-2013 01:54.00 pm	3006	Car stop	
02-10-2013 04:18.00 pm	3001	Power on	
02-10-2013 04:18.00 pm	3000	Handset power	
02-10-2013 04:20.00 pm	3005	Car run	
02-10-2013 04:20.00 pm	3002	Pass	0
02-10-2013 04:32.00 pm	3009	Retest req	
02-10-2013 04:32.00 pm	3002	Pass	0
02-10-2013 04:40.00 pm	3006	Car stop	
02-11-2013 07:30.00 am	3001	Power on	
02-11-2013 07:32.00 am	3003	Abort	
02-11-2013 07:34.00 am	3001	Power on	
02-11-2013 07:35.00 am	3002	Pass	0
02-11-2013 07:35.00 am	3005	Car run	
02-11-2013 07:45.00 am	3009	Retest req	
02-11-2013 07:46.00 am	3002	Pass	0
02-11-2013 08:17.00 am	3009	Retest req	
02-11-2013 08:18.00 am	3002	Pass	0
02-11-2013 08:18.00 am	3006	Car stop	
02-11-2013 08:43.00 am	3000	Handset power	
02-11-2013 09:02.00 am	3014	Serv reset	
02-11-2013 09:03.00 am	3014	Serv reset	
02-11-2013 09:03.00 am	3017	Cal performed	
02-11-2013 09:06.00 am	3017	Cal performed	
02-11-2013 09:07.00 am	3014	Serv reset	
02-11-2013 09:13.00 am	3000	Handset power	
02-11-2013 09:13.00 am	3001	Power on	
02-11-2013 09:16.00 am	3002	Pass	.01
02-11-2013 09:16.00 am	3005	Car run	
02-11-2013 09:24.00 am	3006	Car stop	
02-11-2013 10:41.00 am	3000	Handset power	
02-11-2013 10:41.00 am	3001	Power on	
02-11-2013 10:44.00 am	3001	Power on	
02-11-2013 10:44.00 am	3002	Pass	0
02-11-2013 10:44.00 am	3003	Abort	

NEW YORK

The following are the types of data that are reported by the vendors to program administrators in the state of New York:

- Devices installed at the end of the month.
- Device counts (by county and grand totals)
  - Remaining devices from prior month
  - Installs for the reporting month
  - De-installs from the reporting month
  - Total remaining devices at the end of the month
  - Fee status - number of fully paid, pay plan or waived units
- Negative event counts (by county)
  - Number of failed or missed service visits
  - Number of persons failing or missing a start retest (with number of BRAC readings above 0.08)
  - Number of persons failing or missing a rolling retest (with number of BRAC readings above 0.08)
  - Number of lock-outs (initiated, number of vehicles disabled and number of persons attempting to circumvent or tamper with an installed device)
- Description of any device malfunctions and explanation of actions taken by the manufacturer to correct such malfunctions.
- Number of devices that did not meet calibration standards upon servicing.
- Brief summaries of any owner, vehicular user and installation or service provider complaints.

APPENDIX B – SOUTH CAROLINA'S AUTOMATED DATA MANAGEMENT SYSTEM

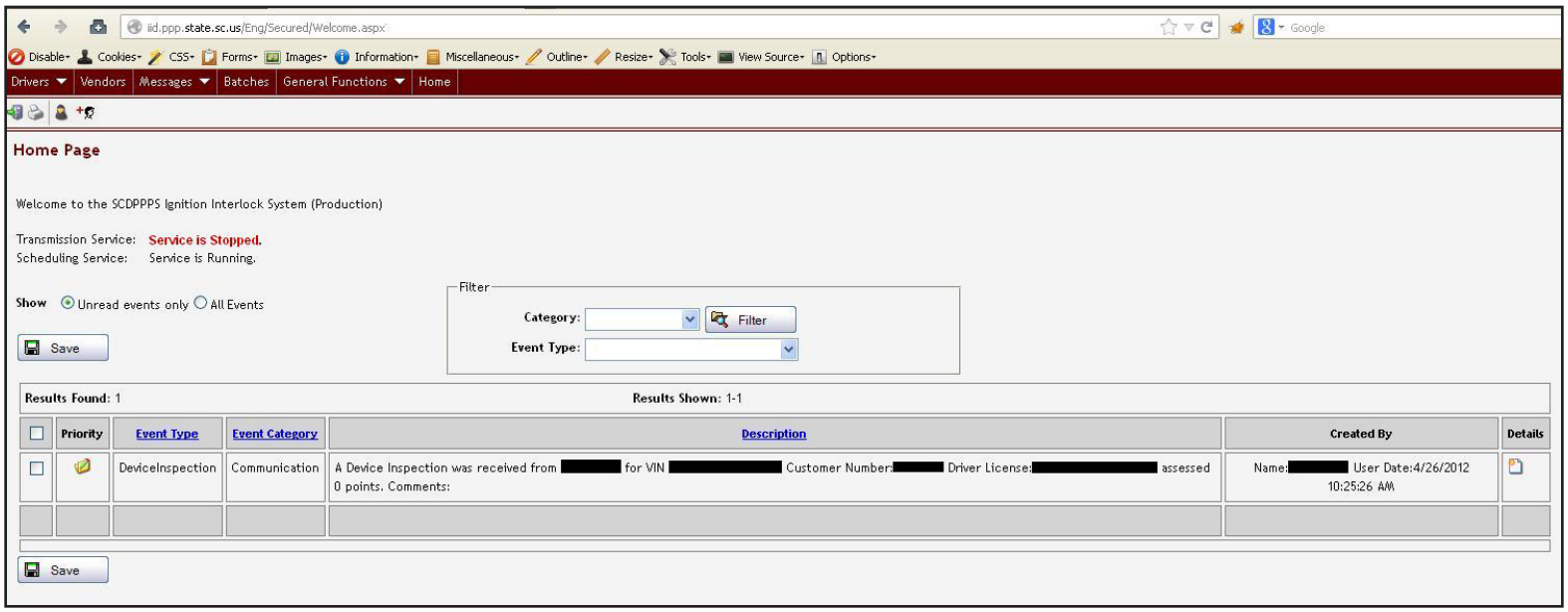
South Carolina has developed a sophisticated software program to manage interlock offender case files. The program is operated by the Department of Probation, Parole, and Pardon Services (PPP) and is interfaced with the DMV to allow information about offenders to be transferred and shared as appropriate. This program enables vendors to send data downloaded from the interlock devices directly to PPP who subsequently notifies DMV when action is required. The program also permits the entry of electronic case notes, provides an updated status of the offender (e.g., active, awaiting, complete, declined, qualified, removed), and indicates any violations. This program further allows PPP to notify DMV when a letter should be sent to the offender in response to non-compliance.

South Carolina's system also facilitates the generation of reports by PPP in relation to offenders. For example, a monthly indigent fund remittance report tracks the amount of money that has been deposited and removed from the indigent fund. PPP also has the capabilities to generate reports detailing the number of offenders in treatment, the number who have completed the program, and in which counties interlocked offenders reside.

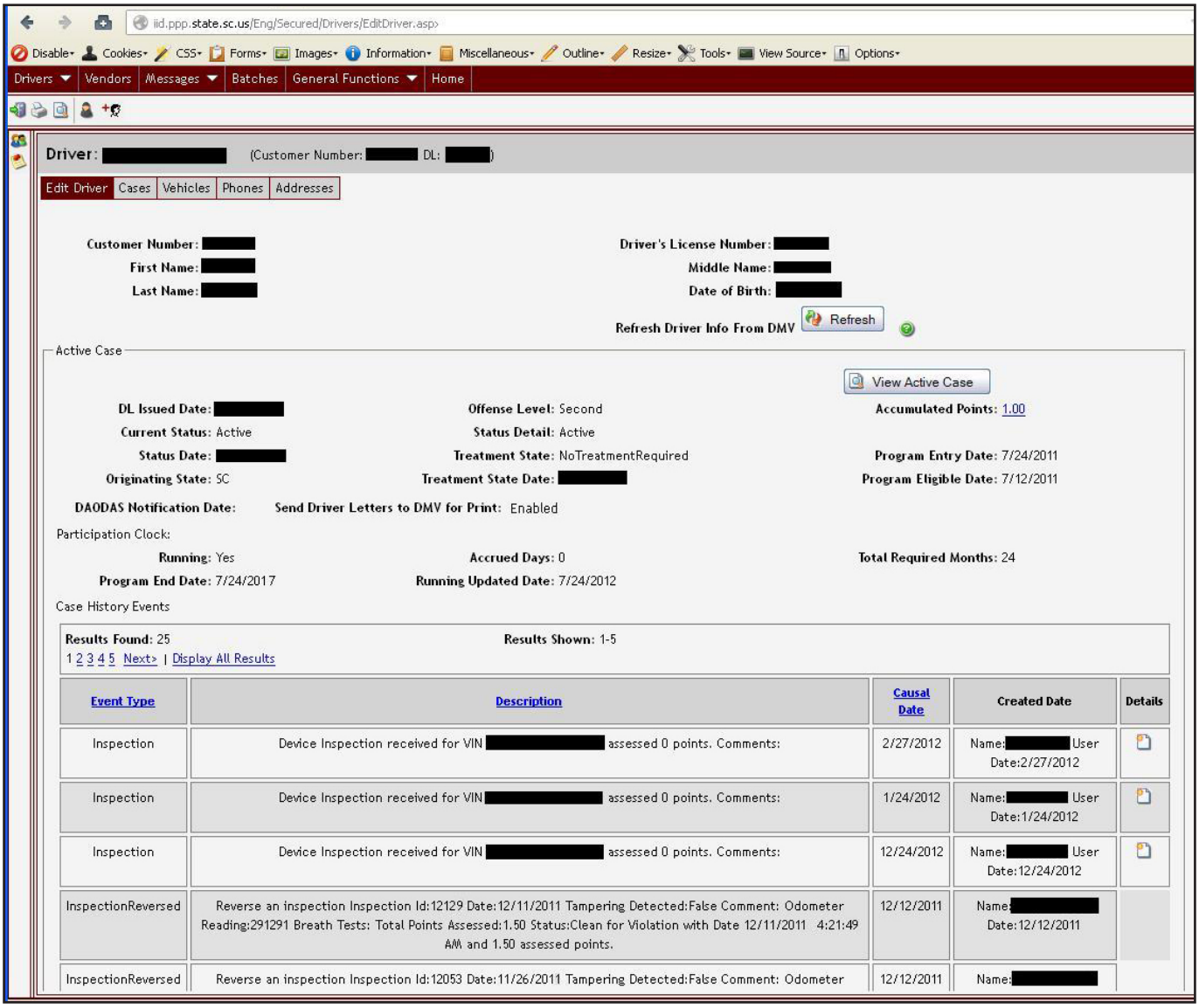
This type of program is a very powerful tool in that it greatly facilitates the monitoring of interlocked offenders and the management of interlock cases. Given its monitoring capabilities, the program ensures that there can be quick accountability for offenders when violations do occur. It is a model that can be utilized by other jurisdictions that are seeking to transition from a paper-based to an automated system.

The following are screenshots that walk through the various aspects of South Carolina's system.

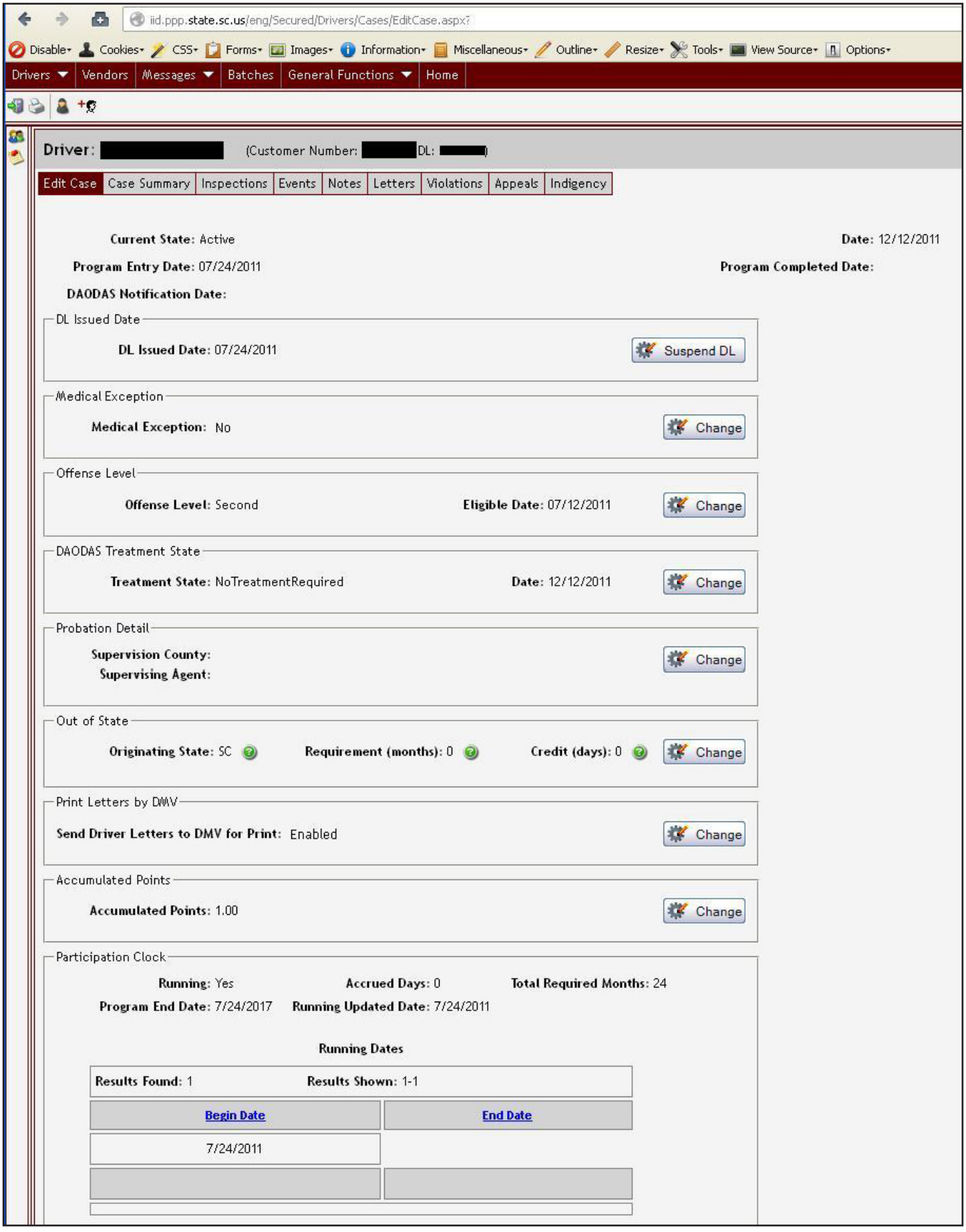
Home Page. This is the main page after logging into the system. It will tell you if the back end services are up or not, and provide a list of all new system activity. An administrator can check off each item as 'Done'. The 'Details' button to the right links directly to the driver, case, or notification event, as applicable. The IID administrator does not necessarily have to do anything with respect to each message - some are informational only - but it does allow them the opportunity to be made aware of all activity.



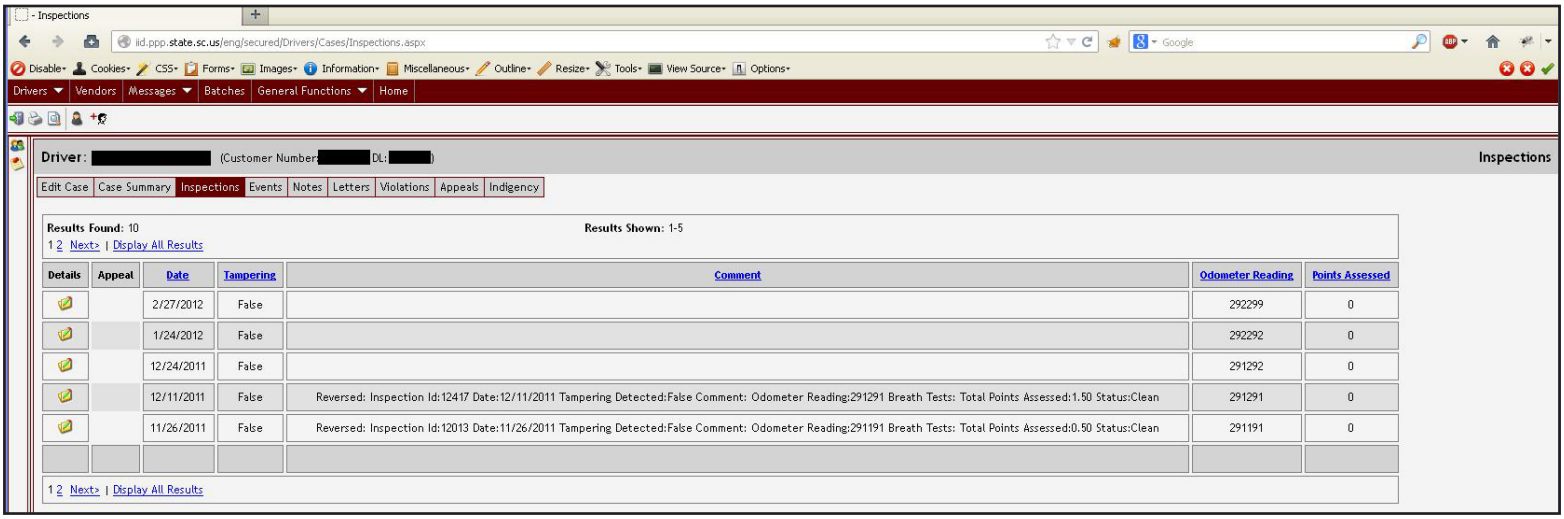
Driver Homepage. This page displays the information for a specific driver. In this case, it is a driver who is actively participating in the program, but the driver could be suspended, pending, closed, etc. If there is an active case then a summary of that information is displayed as well. If there is no active case, then most of the page is empty. Note, it is possible for a driver to have multiple cases, which means they have come through the IID program multiple times. The Driver Homepage assumes that the user is only interested in the current case, and provides a link to the current case. The archived cases can be accessed from the Cases tab at the top of the page. Other driver data such as vehicles they own or have owned, phone numbers and addresses are on their own tabs as well (not shown).



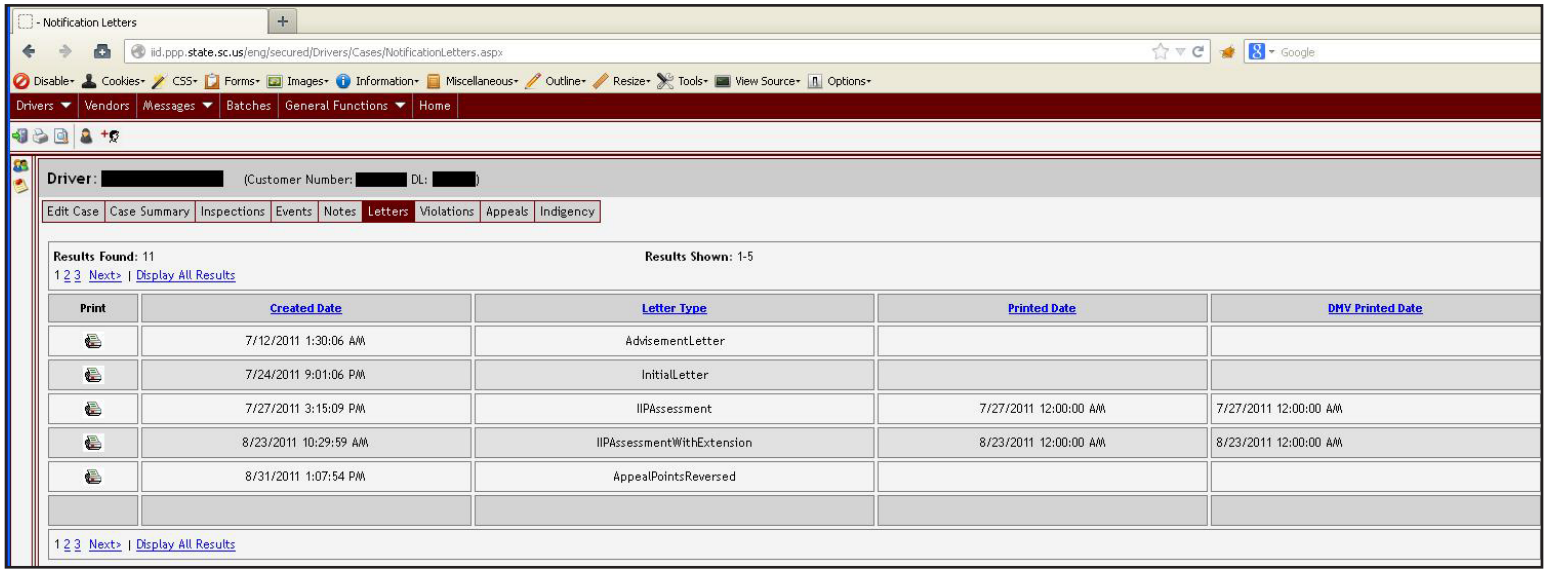
Edit Case. This is the main page for a specific case. This page informs the user when the IID license was most recently issued, the level of the offense (in this case, DUI 2nd), the current status of treatment per the Department of Alcohol and Other Drug Abuse Services (DAODAS), whether the person is also on probation, if they have an IID requirement from another state and have moved here, and how many points they have accumulated in penalty. The last box at the bottom of the page is the participation clock, which is how the system keeps track of starts and stops within the program. If the driver has their license suspended, for example, the clock will be stopped until the driver is issued another IID license.


iid.ppp.state.sc.us/eng/Secured/Drivers/Cases/EditCase.aspx?
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options
Drivers Vendors Messages Batches General Functions Home
Driver: [redacted] (Customer Number: [redacted] DL: [redacted])
Edit Case Case Summary Inspections Events Notes Letters Violations Appeals Indigency
Current State: Active
Date: 12/12/2011
Program Entry Date: 07/24/2011
Program Completed Date:
DAODAS Notification Date:
DL Issued Date
DL Issued Date: 07/24/2011
Suspend DL
Medical Exception
Medical Exception: No
Change
Offense Level
Offense Level: Second
Eligible Date: 07/12/2011
Change
DAODAS Treatment State
Treatment State: NoTreatmentRequired
Date: 12/12/2011
Change
Probation Detail
Supervision County:
Supervising Agent:
Change
Out of State
Originating State: SC
Requirement (months): 0
Credit (days): 0
Change
Print Letters by DMV
Send Driver Letters to DMV for Print: Enabled
Change
Accumulated Points
Accumulated Points: 1.00
Change
Participation Clock
Running: Yes
Accrued Days: 0
Total Required Months: 24
Program End Date: 7/24/2017
Running Updated Date: 7/24/2011
Running Dates
Results Found: 1
Results Shown: 1-1
Begin Date
End Date
7/24/2011

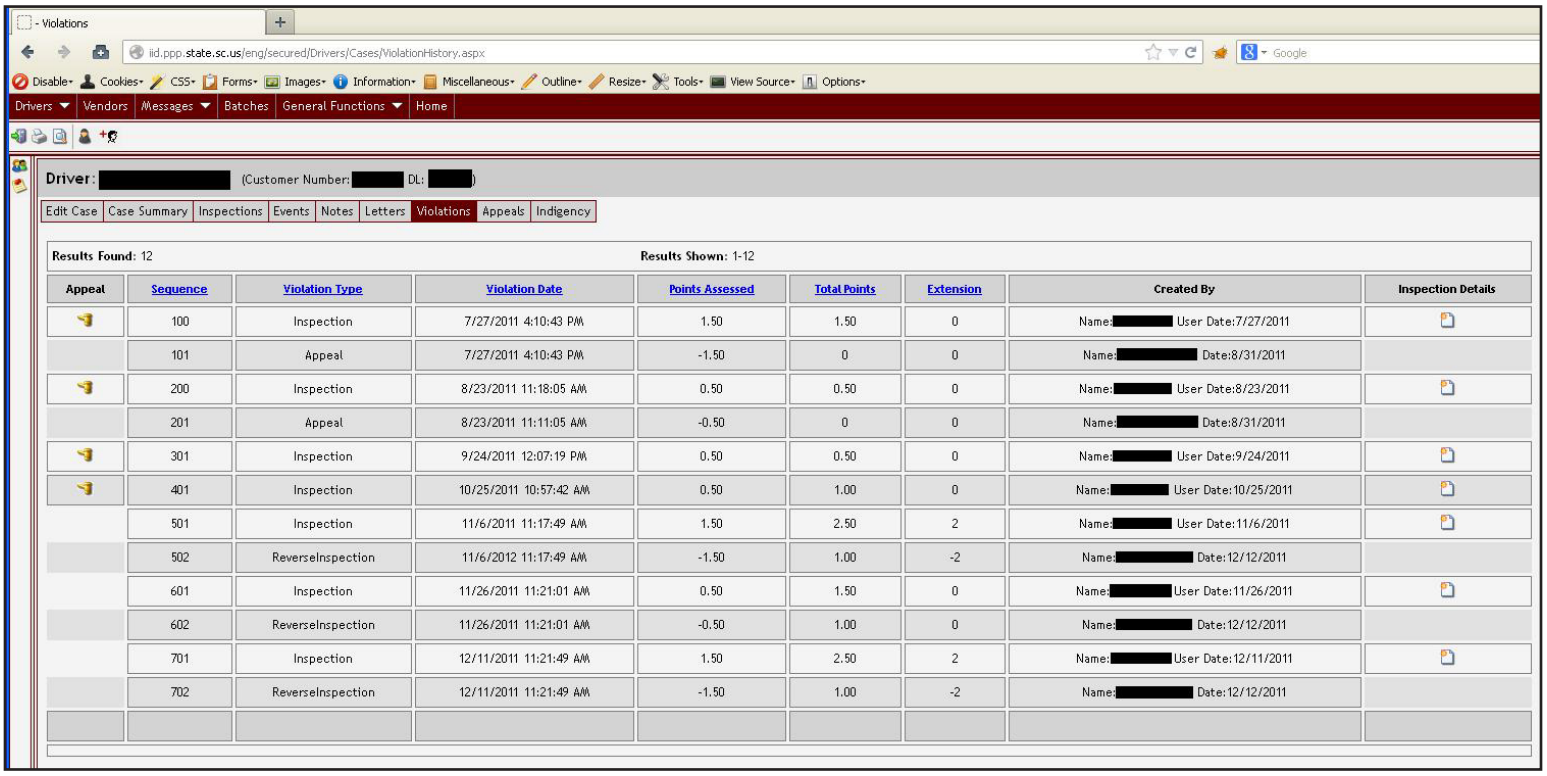
Case Inspections. This page lists all the inspection downloads for a particular case. It covers all vehicles for the driver. For example, if someone owns two cars, each with an IID, then data from both devices will be recorded here. This page is a summary of each inspection and includes any points resulting from the download and whether there were appeals to the points. The administrator can receive additional details on a specific inspection by clicking the icon on the left. Although there is typically little information there since the only data the program retrieves from the vendor are events which generate points, rather than every event for every inspection. In other words, if a driver tried to start a car with a 0.02 BAC, the administrator would see that in the Details tab, but the program would not download every car start attempt. This was simply a design choice to save disk/bandwidth. If the full details of every start attempt are required, they are available on the vendors' websites.



Case Notifications. On this page an administrator can send notifications to the driver at various stages of the program. The system sends letters to the driver when they are first entered into the program, when they have a data download that has points (violations) in it, the results of any appeals they have submitted to the program, and when they are due to complete the program. Because South Carolina's DMV has an automatic letter printing service, the system submits most of its letters to the DMV for batch printing and mailing. The print icon to the left can recreate the letter to be viewed or printed locally, if required.



Case Violation History. This page shows all violations, appeals, and administrative edits. This is similar to the details for a download event, except it is a list of every activity relating to modification of the driver's points. The icon to the right can crosslink to the specific inspection that generated those points, if applicable.



- Violations

iid.ppp.state.sc.us/eng/secured/Drivers/Cases/ViolationHistory.aspx

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

Drivers | Vendors | Messages | Batches | General Functions | Home

Driver: [redacted] (Customer Number: [redacted] DL: [redacted])

Edit Case | Case Summary | Inspections | Events | Notes | Letters | Violations | Appeals | Indigency

Results Found: 12 **Results Shown:** 1-12

Appeal	Sequence	Violation Type	Violation Date	Points Assessed	Total Points	Extension	Created By	Inspection Details
	100	Inspection	7/27/2011 4:10:43 PM	1.50	1.50	0	Name:[redacted] User Date:7/27/2011	
	101	Appeal	7/27/2011 4:10:43 PM	-1.50	0	0	Name:[redacted] Date:8/31/2011	
	200	Inspection	8/23/2011 11:18:05 AM	0.50	0.50	0	Name:[redacted] User Date:8/23/2011	
	201	Appeal	8/23/2011 11:11:05 AM	-0.50	0	0	Name:[redacted] Date:8/31/2011	
	301	Inspection	9/24/2011 12:07:19 PM	0.50	0.50	0	Name:[redacted] User Date:9/24/2011	
	401	Inspection	10/25/2011 10:57:42 AM	0.50	1.00	0	Name:[redacted] User Date:10/25/2011	
	501	Inspection	11/6/2011 11:17:49 AM	1.50	2.50	2	Name:[redacted] User Date:11/6/2011	
	502	ReverseInspection	11/6/2012 11:17:49 AM	-1.50	1.00	-2	Name:[redacted] Date:12/12/2011	
	601	Inspection	11/26/2011 11:21:01 AM	0.50	1.50	0	Name:[redacted] User Date:11/26/2011	
	602	ReverseInspection	11/26/2011 11:21:01 AM	-0.50	1.00	0	Name:[redacted] Date:12/12/2011	
	701	Inspection	12/11/2011 11:21:49 AM	1.50	2.50	2	Name:[redacted] User Date:12/11/2011	
	702	ReverseInspection	12/11/2011 11:21:49 AM	-1.50	1.00	-2	Name:[redacted] Date:12/12/2011	

Regarding treatment, the system does not track very much simply whether the driver is required to participate in treatment and their progress. DAODAS handles the particulars, and informs the PPP of their current status. Some of the calculations regarding who is in the program can get fairly complex. The participation clock will start and stop based on what the PPP, the DMV or the vendors say. The clock has to support retroactive activity, since the PPP might be informed today that a driver's license should be suspended as of a month ago. Not only does the driver need to not be credited for the last month, but any points violations need to be removed from their history, which might in turn reduce their total suspension period. If tomorrow, the DMV informs the PPP that a driver received another IID license the day after it was suspended, the PPP would have to reimplement those points, any extension, and give him credit back. All of these calculations are automatic, so that in most cases the administrator just needs to know that the driver is "done at the end of the month".

APPENDIX C – AUTOMATED DATA MANAGEMENT SYSTEM IMPLEMENTATION CHECKLIST

A. Exploring automation options

- ❑ Did you undertake an audit or inventory of the current existing system and its capabilities?
- ❑ Did you determine if updates to the existing driver records system are required?
  - ❑ Did you determine if resources are available to make these improvements?
  - ❑ Did you ask for a cost estimate for the automation process?
  - ❑ Did you assess whether there are sufficient funds available to develop an automated system?
- ❑ Did you conduct an environmental scan of other available data management systems?

B. Developing an automation plan

- ❑ Did you review any existing interlock data system to collate and manage reports from vendors regarding different classes of offenders?
- ❑ Did you make a list of all of the actions that will be required of the interlock data system with regard to any new classes of offenders?
- ❑ Did you check to ensure that the driver records system has been updated to accommodate for any new classes of interlock offenders (e.g., first offenders)?
- ❑ Did you create a draft list of all of the actions that are expected to be performed by the automated system?
- ❑ Did you review linkages between the driver records system and the interlock data system to accommodate any new classes of offenders?
- ❑ Did you form a working group and assign leadership and other roles?
- ❑ Did you assign a DMV staff person to be actively involved in the development process?
  - ❑ Did you assign a qualified and knowledgeable DMV staff person to oversee and manage contractors?
- ❑ Did you discuss governance policies related to data ownership, access, and sharing?
- ❑ Did you hold an internal meeting of stakeholders to identify current practices and gaps?
- ❑ Did you investigate the structure and accessibility of court and correctional data systems to facilitate the sharing of information and communication among agencies?
- ❑ Did you hold meetings with interlock vendors to gain their input early on in the development process?
  - ❑ Did you explore whether each vendor's respective data management system is able to interface with any new system utilized by the agency authority?
- ❑ Did you determine whether the work will be completed in-house or by contractors?

- ❑ Did you issue an RFP for contractors?

C. Key tasks to complete

- ❑ Did you translate the current system into business rules or workflow?
- ❑ Did you determine what the ideal system would look like?
  - ❑ Did you determine what the scope of the work would be?
  - ❑ Did you translate the ideal system into business rules and workflow?
- ❑ Did you compare business rules and workflow of current system with those of ideal system?
- ❑ Did you agree upon the information that will be included in the new system and shared across agencies and localities?
- ❑ Did you clearly define the criteria and articulate to vendors what pieces of data you want captured and reported?
  - ❑ What data are agencies expected to report?
  - ❑ Who does the data get reported to?
  - ❑ Who is filtering the data?
  - ❑ Who has access to the data and at what level?
  - ❑ How much information will be made public and how much will be protected against disclosure?
- ❑ Did you develop quality assurance protocols and testing protocols to ensure that the new system will work well for all stakeholders?
- ❑ Did you identify agency requirements (e.g., data files, reports, web access, notifications)?
- ❑ Did you involve the judiciary in the process to assess interface capabilities for sharing court case information with driver records?
- ❑ Did you involve other agencies who are peripherally involved in the delivery of the interlock program (e.g., probation or treatment)?

D. Concerns to address

- ❑ Did you estimate the time it would take to automate? Did you take into account the potential for delays in implementation?
  - ❑ Did you get time estimates from staff? From contractors? From both?
  - ❑ Are these timelines regularly updated?
- ❑ Did you take into account privacy, civil liberty, and confidentiality issues when developing information-sharing protocols?
- ❑ Did you discuss the potential for reciprocal arrangements with neighboring jurisdictions?
- ❑ Did you negotiate data-sharing agreements with tribal governments (if applicable)?
- ❑ Did you take advantage of any potential linkages that could be made for indigency provisions (e.g.,

tax records)?

- ❑ Did you consider developing means for tracking the number of offenders deemed unable to afford the interlock?

E. Identifying system requirements

- ❑ Did you identify all hardware and software requirements?
- ❑ Did you determine if the existing server can handle any additional upgrades?
  - ❑ Did you develop some form of contingency should the server be rendered non-operational?
- ❑ Did you confirm that what is built as an interface will work with vendors?
- ❑ Did you investigate what has been built in other jurisdictions that can be used/borrowed/modified to reduce costs?
- ❑ Did you account for technological differences across agencies?
- ❑ Did you create a data back-up and disaster recovery plan?
- ❑ Did you ensure that the system will have the ability to upgrade in the future as needed?

F. Managing the reporting process

- ❑ Did you develop standardized reporting procedures?
- ❑ Did you develop standardized terms (e.g., violation definitions) to promote consistency and uniformity among multiple vendors?
- ❑ Did you create a template for standardized reports?
  - ❑ Who is the audience who will use reports and what do they need?
  - ❑ How can program and client review be facilitated?
- ❑ Did you identify who will be filtering data (vendors or the monitoring agency)?
- ❑ Did you develop a minimum set of recommended filters for data?
- ❑ Did you ensure that messages are well-defined?
- ❑ Did you ensure that messages are guaranteed (delivery and confirmation of receipt)?
- ❑ Did you ensure that a system is in place to address and resolve error messages in a timely fashion?
- ❑ Did you address security concerns?
  - ❑ Did you develop policies regarding the secure transmission of data and communication between vendors and agencies?
- ❑ Did you take into account the need for multiple user profiles and different levels of system access?
- ❑ Did you determine how communication with offenders will occur (e.g., in what format; how timely)?
- ❑ Did you ensure that forms and notices are automatically generated?
- ❑ Did you create flexibility to allow for the examination of violations in greater context?

- ❑ Did you have a discussion with vendors and determine the following:
  - ❑ What data will be collected?
  - ❑ Who will have access to the data?
  - ❑ How will data be received and processed?
  - ❑ Who will filter the data?
  - ❑ What actions will be taken as a result of the data collected?
  - ❑ Where is the data going to be stored?
  - ❑ Who will have ownership of the data?
  - ❑ Who will conduct training (if any)?

APPENDIX D - STANDARDIZED FORM CONSIDERATIONS

The following are vendor suggested considerations for the development of standardized reporting forms:

- Create a program summary report that is specific to client populations (e.g., first versus repeat offenders).
- Create a client summary report that is specific to individual interlock program participants.
- Have both fixed and dynamic text on the reporting form.
  - Examples of fixed text include number of tests, total mileage, program violations, use of emergency override feature, and so forth;
  - Examples of dynamic text include explanations of program violations.
- Create a standardized format for all reporting forms:
  - Vendor information (e.g., name of the service provider, address of service center, name of technician) located in the header;
  - Client information (e.g., name, vehicle information, license plate, registration) at the top of the form;
  - Interlock data reported in the middle;
  - Sign-off information at the bottom of the report noting when the offender is eligible to be removed from the program.
- Include a comment box by the client signature at the bottom of the form to justify any program participation extensions or explain program violations.
- Keep the form in black and white format.
- Consider the use of an internal report to be submitted to the DMV.

NOTES

Traffic Injury Research Foundation (TIRF)
171 Nepean Street, Suite 200
Ottawa, Ontario
Canada K2P 0B4
www.tirf.ca
Toll Free: 1-877-238-5235
Fax: 613-238-5292

Registered Charity No. 10813 5641 RR0001