

IMPROVING DUI SYSTEM EFFICIENCY:

A Guide to Implementing Electronic Warrants

Supported by



FOUNDATION FOR
ADVANCING ALCOHOL
RESPONSIBILITY

THE JUSTICE THINK
MANAGEMENT INSPIRE
INSTITUTE CHANGE

Report prepared by Elaine Borakove & Rey Banks, Justice Management Institute

IMPROVING DUI SYSTEM EFFICIENCY

A Guide to Implementing Electronic Warrants

Executive Summary

Executive Summary

Impaired driving has a profound impact on society and public safety, claiming the lives of innocent victims, causing significant injury, and costing millions of dollars in property damage, medical care, and criminal justice expenditures. Despite a 50% decrease in alcohol-impaired driving fatalities since 1982, more than 10,000 people are killed in alcohol-impaired driving crashes annually (NHTSA, 2017). The growing number of states legalizing marijuana and the spread of the opioid epidemic across large swaths of the country has also given rise to concerns about more drug-impaired drivers and drivers under the influence of multiple substances on the roadways. Clearly, addressing impaired driving must continue to be a national priority.

For law enforcement, prosecutors, and the judiciary to be effective in combatting DUI, they must have effective strategies to support investigation, prosecution, and adjudication. From a law enforcement perspective, the biggest challenge in making an impaired driving arrest is obtaining a blood alcohol concentration (BAC) or evidence of drug use. If the suspect refuses a breath test, or if the officer thinks there may be drug impairment and the suspect refuses a blood or urine test, the officer has little evidence to build the case unless he/she can obtain a warrant quickly. Drug-impaired driving presents additional challenges on account of the rapid metabolization of drugs within the body. The inability to obtain a warrant quickly means that drug concentrations in the body at the time of a blood draw will not accurately reflect concentrations in the body at the time of driving.

Luckily, with the availability of technology, lengthy and time-consuming processes for obtaining search warrants are becoming an anachronism. Electronic warrants (eWarrants) provide a mechanism for officers to obtain accurate BAC or toxicology results in a timely manner. These systems can significantly streamline the arrest process, allowing officers to complete requests in their patrol cars on tablets, smartphones, or computers. This practice reduces the amount of time that officers are off the street and the amount of time between the request, approval, and execution of the warrant. Use of an eWarrant system, in which electronic transmission of the warrant affidavit and judicial approval are done through an online information management system, further streamlines the process.

The automated nature of the content of most eWarrants also results in fewer mistakes and errors in the request, which in turn means fewer warrants are rejected by judges. As such, there is a greater likelihood that a blood test will be obtained, resulting in better case outcomes and more appropriate sentencing. By automating the warrant process, we give law enforcement officers a tool for pursuing justice and ensuring that individuals who drive while impaired are held accountable for their actions.

IMPLEMENTATION GUIDE

The Foundation for Advancing Alcohol Responsibility ([Responsibility.org](https://responsibility.org)) awarded a grant to the Justice Management Institute ([JMI](https://jmi.org)) to create a best practices guide for implementing and using eWarrant systems. JMI conducted a multi-phase study to document effective eWarrant systems consisting of:

- A legislative scan to identify which states permit the use of electronic warrants for searches and/or the establishment of probable cause.
- Web-based focus groups with judges and prosecutors and one-on-one interviews with law enforcement to discuss critical issues related to the implementation and use of eWarrant systems.
- Intensive case studies in five jurisdictions with well-established and diverse eWarrant systems (Maricopa County, Arizona; Delaware; Minnesota; Montgomery and Lubbock County, Texas; and Utah).
- Review of findings and the themes identified in the case studies with a working group consisting of experts in law enforcement, prosecution, court administration, the judiciary, and policy. The working group members also offered insight about the most effective strategies for designing and implementing eWarrant systems, funding and resource allocation, and overcoming common challenges.

The information gathered from these activities led to the development of an implementation guide for practitioners. The guide offers insight into the process of planning, designing, funding, and implementing eWarrant systems and highlights important considerations that can influence decision-making along the way.

LEGISLATIVE FRAMEWORK

All 50 states have legislation governing search and seizure that define probable cause, exceptions to the search warrant requirement, and unique restrictions such as the timeframe for the execution of a warrant or rights if a warrantless search is conducted. In reviewing state legislation, JMI found that 45 states include language (either in legislation or in court rules) allowing the issuance of warrants based on telephonic, video, or electronic affidavits.

If a state is considering the passage of legislation or amending current legislation, there are certain elements deemed to be critical. The actual elements that are desirable in a specific state or jurisdiction will vary based on the type of system used.

- Provision for the transmission of the warrant by electronic means, ideally allowing for flexibility to adapt to emerging technologies by not prescribing the specific electronic or digital methods of transmission.
- Provision for oral testimony by telephone or video to allow officers to be sworn in remotely without having to give the oath in-person.
- Language that addresses the need for recording the oral statement and certification by the judge that the sworn oral statement is a true recording under oath.
- Language that addresses the retention of the recording as part of the record of proceedings.
- Inclusion of sworn statement under penalty of perjury to provide further efficiency (i.e., allowing the officer to electronically sign a penalty of perjury statement in lieu of providing testimony).
- Permission for electronic or digital signature by the officer and the approving judge, judicial officer, or magistrate, ideally allowing for flexibility for emerging technologies, but at a minimum including electronic encrypted digital signatures, signatures affixed by electronic stylus, or typewritten signatures.
- If electronic or digital signatures are going to be permissible, inclusion of language related to identity verification protocols should be included, again without being too prescriptive to allow for flexibility as security protocols evolve.
- Language allowing the reporting of failed tests to licensing agencies, ideally allowing for electronic information exchange between eWarrant systems and licensing agency systems.

PLANNING AND DESIGNING AN EWARRANT SYSTEM

Among the greatest lessons learned from jurisdictions that have implemented electronic warrant systems is the need for robust planning in the design phase. There are four major steps to this process:

Identify and engage agencies and individuals. Central to the planning process is collaboration to help align multiple perspectives with legal issues, processes, and technology. Effective eWarrant systems require input from a variety of stakeholders, both traditional and non-traditional. In each of the jurisdictions studied by JMI, a premium was placed on early collaboration – involving judges, law enforcement, prosecutors, and information technology personnel at the state or county levels – as part of the project management team. There are other individuals though who can provide useful insight on the design of the system and its implementation, including legislators, laboratory technicians involved in the analysis of blood tests, the defense bar, county or state government representatives for the procurement process, state department of transportation/office of highway and traffic safety, traffic safety resource prosecutors (TSRPs), sheriffs and police chief associations, and the state driver licensing authority to name a few.

There are two primary steps that should be taken to engage stakeholders and to build a collaborative project team:

1. Identify the appropriate stakeholder groups
2. Create a system to solicit their input and foster participation in planning

Engage in high-level preparation. Once a collaborative project management team has been identified, a deliberate planning process should be followed, starting first with a series of high-level preparation tasks:

- Clearly state the problem to be solved (i.e., articulate what issues the eWarrant system will address) and define the goals and objectives of the project.
- Decide on a high-level approach – determine who will conduct on analysis of the current process for requesting and issuing warrants; identify who will be the lead organization to manage the analysis; determine whether an existing system already has a built-in solution; designate one agency/entity with the authority and responsibility to address future issues as they arise.

- Know the budget (develop a high-level estimate of costs, using information from other jurisdictions, and possible blind consultation with vendors and consultants early in the planning process).
- Map a planning process in terms of time, resources, and responsible parties.
- Procure technical assistance if using a consultant.

Analyze business processes. Business process analysis is a proven technique for clearly defining needs and solutions to those needs. For an eWarrant system, the analysis will necessarily deal with software, hardware, and processes. The business analysis will typically take between six to nine months. The following steps are commonly used in a business process analysis, tailored to an eWarrant system. The deliverable is often called a business requirements document (BRD), which provides specific details about the solutions that will be implemented for the eWarrant system.

1. Undertake information-gathering (e.g., collect data and gather existing process documentation; conduct interviews and site visits to gather requirements from key stakeholders and users; conduct statutory research).
2. Map the existing “as-is” business processes (e.g., use information gathered to create a narrative description, workflow diagrams, user lists, and data/document indexes and repositories).
3. Map the new, proposed business processes (e.g., complete a business requirements document, requirements traceability matrix, workflow diagrams, business rules, and user roles and permissions).
4. Identify all data and information exchange touchpoints.
5. Catalogue all forms and documents to be automated.
6. Define administrative tools (i.e., identify who requires access and to what degree as well as the particular values or items that need to be included in order to navigate through the system).
7. Specify performance requirements (i.e., anticipate agency decision-maker and frontline staff expectations for system performance and work with system developers to mitigate issues and ensure that the system functions to meet the needs of its users).

Determine technological requirements. A business process analysis for an eWarrant system will need to be paralleled or followed by an analysis of the technological requirements, which should include:

- Involvement of state or county information technology (IT) personnel to help understand what technology options are available currently and what may be needed.
- Consideration of security and privacy issues related to any existing platform or a new platform to be developed, in addition to the design features.
- Identification of what expectations law enforcement, prosecutors, and judges have about how the system should operate, particularly in terms of how they will access and use the system.

Ideally, the eWarrant system can be built onto an existing platform. Beyond the obvious benefit of likely being more cost effective, use of an existing platform can reduce the need for user hardware, benefit from use of existing access and security protocols, and streamline the implementation process. If this is not feasible, a new system must be constructed.

Development of technology requirements can be conducted in parallel with a business process analysis, but should be predicated on business requirements. The following steps are commonly used in the development of technology requirements, tailored to an eWarrants system:

1. Perform technology information-gathering (i.e., document existing technologies and infrastructure including network diagram, network hardware and software (including bandwidth, security, access controls, and operating systems) host systems, end-user hardware and software, and mobile technologies that may be used by law enforcement or other stakeholders).
2. Conduct a technology gap analysis to assess whether the existing network and application technologies will support a solution, or whether the foundational technologies need to be upgraded/supplemented.
3. Define architecture of the new system (i.e., identify the key components and delineate which agencies or entities have ownership of each of these components).
4. Define suite of technologies that will meet the needs for the eWarrant system (e.g., if the jurisdiction is currently using faxed affidavits and warrants, how much will the system simply mirror a document management exchange in digital format?).

FUNDING ELECTRONIC WARRANT SYSTEMS

As with any technology solution in criminal justice, the major questions are, “How much is this going to cost, how is it funded, and who is going to pay for it?” There are no easy answers to these questions, and they will undoubtedly vary from state to state, county to county, agency to agency. High-level preparation should provide early cost parameters that will be refined as a result of understanding the technology requirements highlighted in the previous section.

The type of costs will vary – from hardware and software costs to personnel costs for programming. There may also be costs associated with hiring consultants to conduct business process analyses. A good planning process should take all possible costs into consideration to identify opportunities for multiple funding sources and cost-sharing. Among the jurisdictions studied by JMI, costs for design and implementation ranged from zero (in the case of Delaware in which costs were just absorbed as part of the normal function of the Delaware Justice Information System) to \$350,000 in Minnesota to build an eWarrant module into the state’s e-Charging platform.

The jurisdictions studied used several different funding sources – including state or grant funding, fees for cost recovery, and other low-cost options – to cover the expense of their eWarrant systems. Agencies that are considering developing their own eWarrant system should explore each of these funding strategies to determine their feasibility.

POLICY AND OPERATIONS

A central theme throughout interviews with stakeholders who have implemented eWarrant systems is that consistency ensures reliability and operational policies foster consistency. Although states may have explicit policies enumerated statutorily or through court rule, there are certain key policies that should be considered by jurisdictions seeking to implement or refine electronic warrant systems:

Authentication and security. Even on a secure system, user authentication is paramount for ensuring that judges can identify the law enforcement officers with whom they are dealing and vice versa. Authentication and security risks decrease if the system is both secure and verifiable at each end of the communication and if the network is secure. Authentication and security, then, are categorized on digital systems as user identification and network security.

User identification methods include login authentication, which authenticates a user before access to the system is granted; network access authentication which authenticates both user identity and application access to the network services; and IP security authentication which is necessary for officers and judges to electronically sign warrants. User identification technologies include usernames and passwords, authentication codes, and biometrics. Comparable technologies are used to authenticate electronic signatures by officers on applications and affidavits and by judges on warrants as well as other types of related orders.

Network security is key to determining how secure user identification needs to be. In non-technical terms, if a network is not secure, and access to it is easily compromised, user identification is critical to authentication and security. Network communications between law enforcement and the courts may be provided in a closed network environment, using dedicated, leased lines. But, most network communications today are virtual, or virtual private networks (VPNs), that utilize the public Internet or components of it. Most network security is provided by server authentication and encryption. If there are not current authentication and security protocols in place for other systems that can be incorporated into an eWarrant application, jurisdictions should consider conducting a security needs analysis.

Officer’s oath and swearing to factual statements. One of the challenges to an eWarrant system is the need to take officers’ oaths and have them swear to the facts contained within the warrant. In many places, statute or local rule requires this be done in-person, which can present a barrier to the timely issuance of the warrant. In some jurisdictions, it may be necessary to engage the courts in changing the administrative rules of criminal procedure to allow probable cause statements to be sworn in electronically or digitally as was the case in Utah. In other instances, legislation may need to be changed.

Some of the options identified in the case study jurisdictions and by the expert working group members for addressing oath issues include:

- Adding a penalty of perjury statement on the warrant (i.e., declaring the facts stated in the warrant to be true and correct) which is then signed and dated.
- Allowing the swearing-in to occur over a recorded telephone line or video conference which is permitted in Georgia.

- Allowing law enforcement officers to swear in other law enforcement officers as is common practice in Texas.

Warrant retention. Another policy consideration is how long, and where, pending and executed warrants will be retained. In making determinations about the retention policy, some questions to consider include:

- Are there statutory requirements for the retention of records, specifically warrants?
- Which agency will have responsibility for storing the warrants?
- What is the impact on storage space (largely determined by length of retention policies)?
- For what purposes might someone need access to stored warrants, and who would be authorized to access these documents?

Beyond policy, the expert working group pointed to pilot testing and training as critical elements for ensuring consistency and uniformity in the use of eWarrant systems.

Pilot testing. In an effort to identify potential challenges or issues with a new eWarrant system, many jurisdictions have opted to run a pilot test of the system with a subgroup of offenses or in a single jurisdiction before going fully “live.” Many of the current statewide systems, such as the one in Utah, began in a single jurisdiction with a single law enforcement agency.

The pilot test validates the processes and functionality of the system, identifies potential glitches in the software, and highlights any unforeseen challenges. The pilot test also provides insight into training that will be needed or any areas of additional resistance to change that may need to be addressed. During and following the pilot test, it will be important to collect and assess feedback. Standardized questionnaires to solicit user feedback, along with metrics on system performance, are both useful tools for systemically documenting the pilot test process.

Both user experience and system performance should be analyzed to identify:

- Pervasive issues that may require additional programming or development.
- Aesthetic issues related to layout and format of the online interface.
- Paper documentation that is generated from the system.

- Training needs to provide more clarity for users.

Depending on the scope of revisions identified, particularly those related to reprogramming or development, it may be necessary to conduct additional tests prior to full implementation.

Training. To ensure that users of any eWarrant system are able to navigate the system efficiently, proper training is necessary. The better and more comprehensive the training, the less likely that users will encounter problems, thus minimizing frustration with the process and increasing acceptance and support for the system’s use. Important activities for any eWarrant training initiative include:

- Identify all agencies that may require training and education on system implementation and use.
- Identify which entity will be responsible for developing a training curricula and associated materials.
- Identify who will be responsible for conducting training (i.e., will one individual or entity be responsible or will a train-the-trainer format be used?).
- Develop a standard training curricula and materials to be used by all parties involved to ensure consistency.
- Determine when it is most advantageous to train system users and in what venue.
- Explore the possibility of offering continuing legal education (CLE) credits as an incentive for completing the training.
- Update and augment the training to reflect feedback from system users (i.e., as issues with the system are identified, incorporate these into training to educate users on how to troubleshoot effectively or avoid complications).

Regardless of the training approach employed, all jurisdictions should seek to ensure consistency in educational content and materials. Furthermore, it is recommended that feedback be elicited from practitioners to gauge whether the level of information contained in the training is adequate and to determine whether existing materials require updating and/or augmentation. As common issues with system operation and use are identified, training should be modified to make sure that they are addressed.

MEASURING EFFECTIVENESS

Ongoing assessment of eWarrant and eWarrant system effectiveness is critically important for ensuring the intended goals are being met, and if they are not, measures of effectiveness can help pinpoint areas for improvement. If a jurisdiction is creating an eWarrant system, attention should be given to the types of metrics that can be built into the system as a data dashboard or for regular reporting (e.g., number of system logins; number of warrant requests submitted; number of warrants approved and rejected; average length of time from submission to return of service, etc.).

Other metrics that can be helpful are those that document the user's experience. Although these metrics typically are not built into the system itself, a short annual questionnaire or roundtable at the state law enforcement/judicial conference can be used to collect information (e.g., How easy was it to access the eWarrant? How easy was it to submit the affidavit? Did you encounter any problems when preparing or reviewing an eWarrant?).

Finally, eWarrants are intended to provide law enforcement, prosecutors, and judges with the tools they need to effectively respond to DUI and to hold offenders accountable. These broader outcomes can be measured by tracking information and analyzing change over time (e.g., number of refusals to submit to chemical testing; number of motions made to suppress BAC tests on the basis of probable cause; number of DUI convictions, etc.). Agencies are also encouraged to collect baseline data to be able to show how eWarrant systems improve overall system efficiency and outcomes. For example, showing the amount of time that can be saved by transitioning to an electronic warrant system or reductions in warrant rejection due to errors.

CASE STUDIES

Jurisdictions interested in developing and implementing their own eWarrant system are encouraged to first examine the systems/processes in place in other localities and learn from both the challenges and successes of agencies in other states. Each of the systems studied by JMI have unique features and operate in a slightly different manner; they represent locally-based to integrated statewide systems.

eSearch Warrants in Minnesota

In Minnesota, the courts use a statewide electronic charging system, known as e-Charging, for criminal complaints and to move information between law enforcement, prosecution, courts, and the state driver and vehicle services department. In addition to criminal complaints and search warrants, e-Charging is used for electronic citation processing, DWI processing, and law enforcement incident report submission to prosecutors.

Minnesota prioritized the development of eSearch warrants for blood draws in DWI cases because in addition to court decisions requiring search warrants for blood or urine tests, the state was experiencing a growing number of legal challenges around blood draws and implied consent. These factors combined with a significant increase in blood draw requests and the challenges to obtaining time-sensitive warrants in rural areas provided the needed impetus for the creation of an electronic system.

What to know about Minnesota's system:

- The Bureau of Criminal Apprehension (BCA) was responsible for the planning, design, and implementation of the eSearch warrant application with a \$350,000 grant from the Department of Public Safety's Office of Traffic Safety.
- A collaborative group of stakeholders, including law enforcement, the State Court Administrator's Office, and district court judges, worked together to draft the warrant template.
- The roll-out of eWarrants for DWIs began in October 2016 with a 3-month pilot program, first with the Minnesota State Police in Hennepin County. By mid-November 2016, eight municipal police departments had been added to the pilot, with successive roll-outs across the state by judicial district. By April 2017, the system had gone statewide.
- Officers seeking a warrant for a blood test log onto a secure portal to complete and submit an electronic search warrant application to a judge.
- The system is designed to interface with Driver and Vehicle Services so that the officer can conduct a search based on name and date of birth to confirm the identity of the suspect and auto-populate the demographic fields (e.g., address; driver's license) as well as the vehicle information.



- The on-call judge receives an email with a hyperlink directly to the warrant in the system. After reviewing the warrant, the judge may either issue it by applying an electronic signature or reject the application.
- Experienced officers typically can prepare warrants in 10 minutes or less, and officers report the average processing time, from submission to judicial approval, is between 15-20 minutes.
- Since the eSearch warrant became available, Minnesota law enforcement officers have submitted over 2,500 applications for DWI-related search warrants. Ninety-eight percent of those applications are approved and result in the judge issuing a search warrant. In addition, the error rate on DWI forms has been reduced from 30% to nearly 0%.

Utah Criminal Justice Information System (UCJIS)

The state court system introduced an electronic warrant pilot program in the spring of 2008, in response to a court decision ([State v. Rodriguez](#), 156 P.3d 771 (2007)). The Utah Department of Public Safety (DPS), the Salt Lake City District Attorney's Office, and the Administrative Office of the Courts (AOC), with collaboration from judges, came together to build an eWarrants system to speed up access to warrants in DUI cases. Since more than 90% of state law enforcement is connected to the Utah Criminal Justice Information System (UCJIS), which unifies data from dozens of separate data sources and agencies, the decision was made to incorporate the eWarrants system into the UCJIS platform.

What to know about Utah's system:

- A grant of \$30,000 was provided to DPS to hire a contractor for the additional programming, which was supplemented with additional JAG funds increasing the total grant to \$34,693. Another grant of \$49,511 was awarded to the AOC, although they ultimately only used \$25,250 of the award, to develop the system. Additional and ongoing funding comes from impound fees.
- Patrol cars in Utah are equipped with computer terminals with Internet capabilities that officers use to log into UCJIS to initiate the warrant request. Each officer has an assigned username and security token that is tied to his/her qualifications and training, allowing the hero statement of the officer's training and qualifications to be auto-populated. The remainder of the warrant includes both drop-down menus and text fields to streamline the process and reduce errors.

- The state uses a rotation system for assigning judges to review warrants. When the officer chooses the jurisdiction and county in which the warrant is being issued, the UCJIS system automatically selects one of the on-call judges. The system then generates a text and email message that is sent to the assigned judge to notify him/her there is a warrant pending review.
- The penalty of perjury statement eliminates the need for administering the oath in-person or via video call. Thus, upon receipt of the warrant, the judge can promptly review and affix his/her electronic signature if the warrant is approved and return it electronically.
- The entire process averages 20 minutes from request to judicial approval, although it can take up to an hour. With the implementation of eWarrants, Utah has improved its test submission rate from 77% to 96% (Berkovich, 2015).
- There has also been tremendous buy-in from stakeholders on the use of the electronic warrant system in Utah, especially in rural areas where there is limited access to judges.

eSearch Warrant and eReturn Applications in Maricopa County, Arizona

The development of the eSearch warrant and eReturn Applications for blood draws in DUI cases began in the summer of 2011. The following year, the Presiding Judge of the Superior Court in Maricopa County issued an administrative order authorizing a two-year electronic search warrant pilot. The pilot project became permanent by Local Rule 4.10, effective May 28, 2014. Once the eSearch warrant and eReturn applications were made permanent, it was expanded to include all Department of Public Safety (DPS) law enforcement officers across the state to allow them access to the system.

What to know about Arizona's system:

- The Maricopa County Superior Court and Phoenix Police Department held three informational sessions with law enforcement to collaborate on the design, development of policies, and implementation of the system.
- The Superior Court received grants from the Governor's Office of Highway Safety to develop the software and enhance the law enforcement officer website to include the return of service. The first grant was provided in the amount of \$30,576 to build the software and cover training costs. The second grant was provided by the State Administrative Office of the Courts in the amount of \$87,838 to modify the software to enhance the application for use by DPS statewide.

- The eSearch warrant application was designed and programmed in-house by the court information technology department as part of the court's information system.
- Officers are assigned a serial number to access the application via the Internet. The application includes a series of checkboxes and pull-down menus that allow the officer to indicate the type of offense, qualifications and training, probable cause for the stop, roadside tests administered, suspect behavior, and refusals.
- Judges receive notice of a pending request and can log onto the system into their "work queue," which shows affidavits they have received and their status (i.e., new, in progress, completed).
- The average time to secure an electronic warrant using the Maricopa County system is between 15–20 minutes. Since implementation, there has been a 13% increase in DUI search warrants.
- By June 2018, the software will be modified to allow all 14 counties and all cities in Arizona access to use the DUI eSearch warrant and eReturn applications.
- The costs for automating and incorporating warrants into the DELJIS platform were absorbed into the DELJIS budget as a part of routine system improvements. Thus, the primary cost to the state was for equipment to allow law enforcement to access the system remotely.
- Law enforcement officers access DELJIS and the eWarrant form with a secure sockets layer (SSL) account through the Internet using laptops, tablets, and desktops. Upon logging into the system, officers enter the suspect's name and date of birth. The DELJIS system automatically searches for the individual to find additional information including criminal history and can access the state's department of motor vehicles records.
- Officers complete the remainder of the request using fillable fields on location of incident, actions of the defendant, statements made, and other facts supporting probable cause. A PDF document is produced, which is then faxed to the on-call judge. The on-call judge swears the officer in via video conference. After review and approval, officers receive the signed PDF via fax. Judges use their bar code as an electronic signature.
- DUI blood draw warrants receive priority within the system, and the average turnaround time is approximately 8 to 10 minutes.

Delaware Justice Information System (DELJIS)

Delaware was the first state to implement an integrated criminal justice information system that supported electronic sharing of criminal justice information among the criminal justice community. DELJIS has been in existence since 1983, and it is constantly changing to meet the needs of system participants, including law enforcement. eWarrants was built into the DELJIS platform, making Delaware one of the first states to use automated warrants.

What to know about Delaware's system:

- Delaware implemented an automated warrant system in 1991, allowing law enforcement to enter complaint data through a mainframe system using Microsoft Word fillable forms to create warrants online. DELJIS later converted the Microsoft Word form into a PDF and housed it on its system. The request for adding blood draw eWarrants to DELJIS was accelerated through the issuance of a policy memo by the Chief Magistrate.
- The design and implementation was a collaboration of the courts, DELJIS, the state prosecutor, and state and local law enforcement.

Electronic Warrants in Texas

Texas does not have a unified court system; each of the 254 counties is responsible for their own criminal justice and court systems, resulting in a patchwork of practices, policies, and results. Several jurisdictions in the state have worked to implement eWarrants. Two counties – Montgomery County and Lubbock County – have implemented eWarrants as a tool to enable the state's No Refusal program.

What to know about Montgomery County's system:

- The Montgomery County District Attorney (DA) worked with Document Logistix, a document management company, to create the application called Mynorefusal.com – a low cost eWarrant which is available at no charge to those wishing to use it.
- Officers log into mynorefusal.com, either by phone or laptop, and using a series of drop-down menus and open text fields provide details about the alleged offense, evidence, results of SFSTs, and other factors relevant to establishing probable cause. The warrant is then signed electronically (typed name followed by "/s") or written by hand on the computer screen if touch screen capability exists.

- Once signed, the system generates a PDF document which is transmitted to a judge by email or fax. The judge receives an email and a phone notification of the pending warrant for review.
- Since the eWarrant capability has been developed, there has been a significant decrease in the number of individuals who refuse breath or blood tests.

What to know about Lubbock County's system:

- The Lubbock electronic warrant system was established in 2012 with a trial period which lasted about 6 months.
- The Lubbock police department trained both officers new to the procedure and judges on the electronic warrant system. Lubbock encountered no significant costs associated with implementing electronic warrants other than the time the officer spent learning the system.
- Once an officer has made a stop and determines probable cause exists to request a blood draw warrant, the officer will write an affidavit on a department issued tablet. The affidavits are standard forms with drop-down menus, as well as text fields.
- Once the judge receives a call, or email alert, that there is an affidavit for review, the judge retrieves it in a PDF document. After it is approved, the judge affixes his/her signature and includes a printed name, date, and time. The approved warrant is then faxed or emailed back to the officer.
- On average, warrants in Lubbock County are being processed within 5 to 10 minutes.
- Following the successful implementation of the system, other law enforcement agencies expressed an interest in using the warrant process created by the Lubbock District Attorney.

TROUBLESHOOTING AND MITIGATING UNINTENDED CONSEQUENCES

The implementation of new processes and systems inevitably produces some challenges as well as unintended consequences. Knowing what challenges may arise early in the design and implementation stages can help offset long-term impact as well as mitigate any unintended consequences.

Troubleshooting. Although it is impossible to predict every conceivable challenge a jurisdiction may face when implementing an eWarrant system, there are several common issues that jurisdictions studied by JMI experienced. These include:

- **Outdated computer systems** - many criminal justice agencies, and courts in particular, operate on legacy systems. These antiquated systems rely on old technology, old programming and methods, and adding new features or creating bridges to access data is almost impossible.
- **Resistance to new technologies** - frontline staff as well as supervisors in law enforcement, prosecutors, and judges may be reluctant to try new systems and technologies. Reasons for their reluctance can vary from simple discomfort or unfamiliarity with new hardware to poor experiences with new technologies that historically have negatively impacted workload. Early engagement of individuals who will use the system is imperative to identify their expectations, needs, and concerns. This is the first step in preparing for resistance and devising a strategy to manage and/or overcome stakeholder apprehensions.
- **Lack of consensus about the format of the eWarrant form** - building consensus among judges about how the final form should be laid out on screen, what it would look like in printed form, where signature boxes would be, and so on has been a larger challenge than foreseen by many. As with overcoming resistance, early involvement of judges in the planning and development phases is important to identify format concerns and work towards a reasonable solution that would satisfy most.

Unintended consequences. While it is not possible to foresee every potential challenge that will arise post-implementation, proper preparation and planning can minimize problems. The involvement of a diverse range of stakeholders at this phase is key to obtain a multitude of perspectives on how the eWarrant system could potentially affect decision-making and the ability of practitioners to perform their jobs. The lessons learned in five jurisdictions studied by JMI, as well as information provided by the expert working group, provide insight into how to mitigate common unintended consequences.



1. Decrease in DRE evaluations.

With the implementation of eWarrant systems, law enforcement officers have confidence they can obtain a chemical sample from a suspect in an expeditious manner. As a result, there is increased reliance on the blood alcohol concentration being admitted as evidence in court. Similarly, the ease in acquiring a blood draw can lead to a false sense that any drug use will also be captured and admitted into evidence and it is no longer necessary to rely on a DRE's opinion. Overreliance on blood testing to make a case instead of relying on extensive documentation of the signs and symptoms of impairment that are part of a DRE evaluation can result in a weaker case. Another drawback in this scenario is if DRE evaluations are not performed, there may be no findings to support polysubstance-impaired driving even if an officer assumes a blood test will provide sufficient evidence.

To address this problem of officers forgoing the DRE evaluation, Utah has incorporated eWarrant training and the continued need for DRE evaluations into its DRE school to ensure not only officers, but also prosecutors and judges continue to recognize the value and merit of the DRE evaluation.

2. Increase in lab turnaround time for blood test results.

This unintended consequence was experienced by nearly all the jurisdictions studied, with return times increasing from as little as 2-3 weeks to as much as 3-4 months or longer. Among the reasons for the longer return times noted by the expert working group were the increased volume of samples being submitted for testing as well as the requirement of technicians to testify in court, which reduces the amount of time they have available in the lab. To reduce the burden on the laboratories, Utah as well as other jurisdictions, have relied on the rules of criminal procedure, which allow for video testimony from experts.

BEST PRACTICES AND LESSONS LEARNED

Regardless of whether a jurisdiction opts for implementing a fully-integrated system or simply automates the warrant, there are a number of lessons learned that can be applied. Individuals involved in the development of the most effective eWarrant systems shared the following strategies that ultimately laid the foundation for successful implementation:

- **Agency leadership** – identify the agency that will take the lead in the development and implementation of the eWarrant system. This agency will assume responsibility for coordinating efforts, convening stakeholders, and maintaining communication throughout the process.
- **Early and consistent stakeholder engagement** – identify and convene the right people as early in the process as possible. Stakeholders should not be limited to those in the lead agency or law enforcement; instead, input should be sought from a diverse range of individuals representing various facets of the DUI system. Communication with stakeholders should continue throughout the planning, development, and implementation phases to elicit feedback and obtain buy-in.
- **Identification of system needs** – determine what the new system will look like and how it will improve upon existing practice to guide system development. To accomplish this task, the lead agency should clearly state the problem to be solved and develop a series of goals and objectives. A high-level approach to preparation will allow the agency to make decisions based on thorough information-gathering.
- **Identification of funding sources** – develop a high-level estimate of costs for system development and implementation and include contingencies in the budget. If the system is to be used by multiple agencies, there may be shared costs and opportunities to reduce the financial burden on the lead agency. Various funding sources should be explored (e.g., state or grant funding, fees for cost recovery, and other creative solutions) to determine their viability.
- **Input from frontline users** – engage with individuals who will be using the system on a consistent basis to obtain their feedback on whether their needs and expectations will be met. By including them in the process, additional challenges that may not have been considered can be identified and resistance to change can be overcome.

- **Pilot testing** – start small when rolling out any eWarrant system and pilot the technology with a single agency. This initial testing period provides an opportunity to build support for the new process/system and to address any user or technology issues before they create frustration.
- **Consistent training** – develop comprehensive and consistent training to prepare users to seamlessly navigate the eWarrant system. There are multiple approaches to training that are commonly used including self-guided training, in-person training, online help resources; jurisdictions are encouraged to use the approach that will be best received among the target audience and to update content as necessary.
- **Use of device agnostic technology** – ensure that the technology chosen allows the user to access the eWarrant on different types of systems (e.g., Windows, Mac, Apple iOS, Android) and hardware (e.g., smartphone, tablet, laptop, or desktop computer); this also creates flexibility for adapting to new technologies as they emerge.
- Addition of a penalty of perjury statement on the warrant to allow for statements to be sworn in electronically or digitally as opposed to in-person.
- Inclusion of a pull-down menu of reasons for rejection if the warrant is denied, along with the option for text input, which not only allows the officer to see the reason for denial and potentially correct it, but also serves as a source of data for additional training if common mistakes are being made by officers.
- Real-time tracking and data analytics that allow officers and judges to see the warrant status and allow system administrators to run reports on system use and outcomes.

Lastly, ongoing review and updates to eWarrant systems is a practice that practitioners agree is of vital importance. By capturing system analytics and tracking change over time, the benefits of the system can be quantified.

CONCLUSION

Although the process for designing and implementing eWarrants can be time-consuming and seemingly complex, the bottom line is that whatever system is adopted, it should be user-friendly and make the DUI arrest process more efficient. By following the steps outlined in this report, agencies can replicate the success experienced in other jurisdictions and learn from the challenges they faced. Through proper planning, stakeholder engagement, pilot testing, and training agencies can implement and expand eWarrant systems.

Once designed, there are a number of key policies and operational practices that have demonstrated significant positive results in DUI enforcement and adjudication. These include:

- Checkboxes or prompts to ensure completeness and accuracy of information being submitted.
- Incorporation of pre-populated information for such items as officer hero statements (summarizing qualifications and training), driver's information, etc.
- Inclusion of open text fields to allow officers to add a narrative or observations as necessary.
- Automated judicial assignment based on the location the warrant is being requested (alternatively, several jurisdictions use a pull-down menu that shows available judges).

¹ For the purposes of this guide, an eWarrant is defined as simply a computerized version of the search warrant affidavit and judicially approved warrant. As discussed in this guide, eWarrants range from a very simple Microsoft Word document or an Adobe Acrobat file (PDF) to an online, fillable form. The process by which eWarrants are stored and transmitted is known as the eWarrant system.

² A BRD details the needs and goals related to the eWarrant system, the processes required to meet these needs/goals, the factors that will influence what is built and why, and documentation of user needs and expectations.

³ A RTM links the business requirements in the BRD throughout a validation process that tests all the requirements of the system.



Contents

Executive Summary	i	SECTION 6	
Glossary of Terms	xiv	Measuring Effectiveness	32
SECTION 1		SECTION 7	
Introduction	1	Case Studies	34
Impaired Driving: Scope of the Problem	1	eSearch Warrants in Minnesota	34
The Challenge for the Criminal Justice System	2	Utah Criminal Justice Information System (UCJIS)	41
The eWarrant Solution	3	eSearch Warrant and eReturn Applications in Maricopa County, Arizona	44
Introduction to the Guide	4	Delaware Justice Information System (DELJIS)	48
Development of the Guide	4	Electronic Warrants in Texas	49
Guide Components	5	SECTION 8	
SECTION 2		Troubleshooting and Mitigating Unintended Consequences	53
Legislative Framework	8	Troubleshooting	53
Summary of Legislation	8	Unintended Consequences	54
Critical Legislative Elements for Successful Implementation	10	SECTION 9	
Model Legislation Checklist	11	Best Practices and Lessons Learned	57
SECTION 3		CONCLUSION	61
Planning & Designing an Electronic Warrant System	13	REFERENCES	63
Stakeholder Engagement and the Collaborative Project Management Team	13	APPENDIX A	
Step 1: Identify Stakeholders	14	Expert Working Group Members & Reviewers	65
Step 2: Create a Plan for Soliciting Input	14	APPENDIX B	
Change Management	15	Legislative Matrix	68
High Level Preparation	16	APPENDIX C	
Business Process Analysis	17	Business Process Analysis Resources	78
Technology Requirements	19	Business Requirements Document Sample (including workflow diagrams and document indices)	78
SECTION 4		Requirements Traceability Matrix Sample/Template	79
Funding Electronic Warrant Systems	23	APPENDIX D	
State or Grant Funding	23	Sample RFP From Washington State Patrol	81
Use of Fees for Cost Recovery	24	APPENDIX E	
Low Cost Options & Alternative Funding Sources	24	Sample Training Materials	83
SECTION 5		Minnesota Electronic Search Warrant Training Materials	83
Electronic Warrant Systems: Policy And Operations	26	Lubbock, Texas Powerpoint for Judicial Training	83
Authentication and Security	26	Utah Dre Training Materials	83
Officer's Oath	27	APPENDIX F	
Retention	28	eWarrant System Resources And Visuals	85
Pilot Testing	28	Minnesota eSearch Warrant Screen Shots	85
Training	29	Utah Criminal Justice Information System eWarrant Module Screen Shots	88
		Texas Mynorefusal.com Screen Shots	95
		Maricopa County Electronic Search Warrant Pilot Program Administrative Order	96

IMPROVING DUI SYSTEM EFFICIENCY

A Guide to Implementing Electronic Warrants

Glossary of Terms

Glossary of Terms

Business requirements document (BRD)

A document that details the needs and goals related to the eWarrant system, the processes required to meet these needs/goals, the factors that will influence what is built and why, and documentation of user needs and expectations.

Customized-off-the-shelf (COTS) software

A commercially available software program that can be purchased and customized to meet system needs.

Device agnostic technology

Software and applications that can be used across different operating platforms (e.g., Windows, Apple, iOS, Android, etc.).

Document management software

Software that is used to track, manage, and store documents.

eWarrant

A computerized document (such as a Microsoft Word or Adobe Acrobat PDF) or form containing the search warrant affidavit.

eWarrant system

An automated process for the electronic storage and transmission of warrant affidavits.

Hardcore drunk driver

An individual who drives with a high BAC of .15 percent or above, or who drives repeatedly with a .08 percent or greater BAC, as demonstrated by having more than one impaired driving arrest, and is highly resistant to changing [his/her] behavior despite previous sanctions, treatment, or education.

Hero statement

A list of police officer qualifications and experience, including all training and experience pertinent to the crime for which the warrant relates.

Requirements traceability matrix (RTM)

A document that links business requirements throughout the validation process. The purpose of the Requirements Traceability Matrix is to ensure that all requirements defined for a system are tested.

Software as a service (SAAS)

The contracted services of a software developer to create a customized system that is unique to the jurisdiction's needs.

Workflow diagram

A flowchart that depicts the flow of tasks or actions from one point in a system to another point in a system that defines how the process works.



IMPROVING DUI SYSTEM EFFICIENCY

A Guide to Implementing Electronic Warrants

SECTION 1

Introduction

SECTION 1: Introduction

For most officers, the biggest challenge in making an impaired driving arrest is obtaining a blood alcohol concentration (BAC) or evidence of drug use. If the suspect refuses a breath test, or if the officer thinks there may be drug use and the suspect refuses a blood or urine test, the officer has little evidence to build the case unless he/she can obtain a warrant quickly. Drug-impaired driving presents additional challenges on account of the rapid metabolization of drugs within the body. The inability to obtain a warrant quickly means that drug concentrations in the body at the time of a blood draw will not accurately reflect concentrations in the body at the time of driving.

Absent toxicology results documenting the suspect's BAC level, the most compelling evidence for judges is video from dashboard and body worn cameras that documents overwhelming evidence of impairment. Unfortunately, video is not always available or usable, and without lab results, convictions for driving under the influence (DUI)¹ become extremely difficult to obtain. For officers on the street, however, getting a warrant for a blood draw can take a significant amount of time—particularly for officers in rural or remote areas where it can take 30 to 60 minutes (or more) just to get to a judge to sign a warrant.

Electronic warrants (eWarrants) provide a mechanism for officers to obtain accurate BAC or toxicology results in a timely manner and help ensure that DUI offenders are held accountable. But these are not the only benefits. DUI cases are also won and lost on arguments of probable cause. To obtain a warrant, an officer must establish convincing probable cause. With eWarrants, the process is streamlined, reducing the potential for errors and omissions, thereby assisting in the case later in court should the element of probable cause be challenged. In the end, eWarrants can decrease the time needed for officers to process an arrest, reduce the number of case continuances in court, and ensure a greater number of convictions.

Beyond arrest and prosecution, BAC and toxicology results provide judges with much more information about the types of assessments that defendants need, particularly if there is polydrug use, to ensure that the appropriate sanctions and treatment are given. Further, the use of eWarrants can have a deterrent effect by educating the public that officers can easily obtain warrants for blood draws if a suspect refuses testing, increasing the likelihood of conviction. This is likely to be a significant game changer for repeat offenders who use

refusals to try to beat the system. The deterrent effect given the likelihood of conviction can, in turn, reduce incidences of DUI overall and further reduce injuries and deaths related to impaired driving.

It is incumbent on law enforcement, prosecutors, court administrators, judges, and policymakers to pursue effective strategies for reducing DUI. First-time offenders and hardcore drunk and drugged drivers, in particular, pose a serious threat to public safety and create considerable societal costs both locally and nationally. By automating the warrant process, we give law enforcement officers a streamlined tool for pursuing justice and ensuring that individuals who drive while impaired are held accountable for their actions.

—**Steven Casstevens**, Chief of Police, Buffalo Grove Police Department, Buffalo Grove, Illinois and **Darrin Grondel**, Director, Washington Traffic Safety Commission, Olympia, Washington

IMPAIRED DRIVING: SCOPE OF THE PROBLEM

Impaired driving has a profound impact on society and public safety, claiming the lives of innocent victims, causing significant injury, and costing millions of dollars in property damage, medical care, and criminal justice expenditures. Despite a 50% decrease in the number of alcohol-impaired driving fatalities since 1982 (Responsibility.org, 2017), more than 10,000 people are killed in alcohol-impaired driving crashes annually (NHTSA, 2017). Alcohol-impaired traffic fatalities, injuries, and damages alone contributed to a cost of \$44 billion per year in 2010, the most recent year for which cost data were available (NHTSA, 2017). This estimate is low, however, as these costs do not take into account the costs of law enforcement patrols and investigation, prosecution, adjudication, defense, punishment, and/or treatment, which are substantial. The growing number of states legalizing marijuana and the spread of the opioid epidemic across large swaths of the country has also given rise to concerns about more drug-impaired drivers and drivers under the influence of multiple substances on the roadways.

Clearly, addressing impaired driving must continue to be a national priority. The Centers for Disease Control (CDC), as part of its Behavioral Risk Factor Surveillance System, examined the prevalence of alcohol-impaired driving among adults in the

United States, aged 18 or older. The study found that in 2012, 4.2 million adults in the United States reported driving while impaired at least once during the 30-day period preceding the study; 40% of these individuals reported driving while impaired more than twice in a 30-day period (Jewett, 2015). This translates into approximately 121 million alcohol-impaired driving instances a year, which is a staggering number even in the face of decreasing fatalities. And yet, the magnitude of the problem may indeed be much greater as self-reports typically under-represent the actual incidences and may not reflect instances of driving while under the influence of marijuana, opiates, and other drugs, alone or in combination with alcohol.

From a public safety standpoint, there are more than a million arrests for DUI each year (FBI, 2016) but these arrests account for only about 1% of the 121 million self-reported episodes of drunk driving nationally (Jewett, 2015). Even with tougher laws and increased enforcement efforts, a significant amount of drunk driving goes undetected. It has been estimated that a driver would have to drive impaired at least 200 times before being arrested once (Beck, 1999). And for those who are arrested, it is often not the first time they had driven while impaired. Approximately one-third of drivers arrested for DUI had at least one prior conviction for driving while intoxicated (Fell, 1995). Among offenders in jail for DUI offenses, 34% reported having three or more convictions, as did 8% of offenders on probation (Maruschak, 1999). Among drivers involved in alcohol-related fatal crashes, 7% had a prior DUI conviction within the three-year period preceding the crash (Responsibility.org, 2016). Moreover, studies have found that hardcore drunk drivers² average 7.1 convictions for driving while intoxicated (Siegal et al., 2000).

THE CHALLENGE FOR THE CRIMINAL JUSTICE SYSTEM

For law enforcement, prosecutors, and the judiciary to be effective in combatting DUI, they must have effective strategies to support investigation, prosecution, and adjudication. DUI cases present a host of challenges for the criminal justice system including refusals to perform the standardized field sobriety tests (SFSTs), refusals to submit to breathalyzer tests and blood draws, as well as incomplete or erroneous paperwork.

Of particular note is the BAC test, as it is viewed by prosecutors and judges as being the single most critical piece of evidence need for conviction, and yet it is evidence that they are frequently without (Robertson, 2002). Law enforcement



What Practitioners are Saying about eWarrants...

“In my jurisdiction, we have a 95% conviction rate in DUI cases, in part because defense attorneys are now advising that people submit to the breathalyzer test rather than face a search warrant for a blood draw.”

—*Warren Diepraam, District Attorney, Waller County, Texas*

“Processing a DUI arrest can be time-consuming, taking the officer off of the street. eWarrants that can be completed in patrol cars allow the officer to obtain search warrants quickly, often within a few minutes, and reduce the time required to complete the arrest.”

—*Chief Steven Casstevens, Buffalo Grove, Illinois Police Department*

“eWarrants, using standardized forms, provide for consistent gathering of evidence, as the forms prompt the officers to provide information necessary for the magistrate to make a proper determination of probable cause. They also assist the magistrate by allowing him or her to quickly get to the heart of each warrant application. By having the boiler plate information pre-printed on the form, there is less opportunity for the officer to make mistakes, which lets them focus on providing detailed information about the reason for the stop and signs of intoxication observed.”

—*Judge Mark Hocker, County Court of Law No. 1, Lubbock, Texas*

note that obtaining a BAC level is the biggest challenge in DUI cases. Offenders, particularly hardcore drunk drivers, know how important this evidence is, and refusals have become a major obstacle to holding drunk drivers accountable. In fact, Jones and Lacey (2000) found that up to 50% of drivers with a prior DUI conviction refuse to submit to a BAC test. Without BAC test results, case outcomes often hinge on the totality of the remaining evidence much of which relies on officer observation and documentation (i.e., driving pattern, slurred speech, bloodshot eyes, SFST performance, video documentation, refusals, etc.). But, such evidence, without chemical test results, may not be of sufficient quality to provide the evidence of intoxication that is needed to convince jurors, making the likelihood of conviction less certain.

Prior to the U.S. Supreme Court decision in *Missouri v. McNeely*, 579 U.S. 41 (2013), law enforcement officers (including prosecutors) and judges believed that officers could forcibly collect blood samples under the exigent circumstances exception to the Fourth Amendment warrant requirement on a per se basis because alcohol quickly metabolizes within the body and it took a lengthy period of time to obtain warrants. In *McNeely*, however, the Court recognized that modern technologies have made it faster and easier for officers to obtain warrants and, therefore, rejected the argument that exigent circumstances **always** exist in DUI cases. The court stopped short of addressing viability of the nation's Implied Consent laws. As such, local practice with regard to obtaining warrants continued to vary, and many states continued to enforce laws criminalizing refusal to submit to chemical testing.

In *Birchfield v. North Dakota*, 136 S.Ct. 2160, 579 U.S. ____ (2016), the Court expanded upon the *McNeely* ruling and held that states cannot criminalize refusals to submit to blood testing in the absence of a warrant or exigent circumstances. However, the Court declined to extend the ruling to breath testing since breath testing is non-invasive. Unfortunately, there are cases in which breath testing is not an option, such as when drivers are injured and taken to medical facilities or cases in which drug impairment is suspected. Further, even states that typically rely on breath testing in misdemeanor cases usually utilize blood tests for drivers who cause crashes resulting in serious bodily injury or death. Given the importance of determining impaired driver's BAC levels, it is incumbent on the states to identify strategies that allow for prompt and effective issuance of warrants for suspects who refuse to consent to BAC testing.

The need to obtain search warrants raises the specter of incomplete or erroneous paperwork. Omissions or errors in search warrants affect both the processing of the arrest and likelihood of conviction, particularly when these incompletions and errors arise in the establishment of probable cause. Improper or incomplete documentation of the officer's observations and reasons for the initial stop, failure to fully complete the police report, and administrative errors (typographical errors, inaccurate descriptions, etc.) can result in delays in the timely processing of warrants. When such errors occur, the amount of time that passes in the attempt to obtain a warrant allows more time for suspects' BAC or drug nanogram levels to drop. Moreover, these types of errors open the door for defense challenges.

THE eWARRANT SOLUTION

With the availability of technology, lengthy and time-consuming processes for obtaining search warrants are becoming an anachronism. In the U.S. Supreme Court's *Birchfield v. North Dakota*, 579 U.S. ____ (2016), which clarified the limits placed on law enforcement, the Court noted that the availability of technology and the possibility of electronic warrants allows for the issuance of timely warrants, negating the exigency argument.

For the purposes of this guide, an **eWarrant** is defined as simply a computerized version of the search warrant affidavit and judicially approved warrant. As discussed in this guide, eWarrants range from a very simple Microsoft Word document or an Adobe Acrobat file (PDF) to an online, fillable form. The process by which eWarrants are stored and transmitted is known as the **eWarrant system**.

“

“In Minnesota, with paper warrants, the error rate on DWI forms was approximately 30%, but with eDWI processing, that rate has now dropped to almost 0%.”

—**Kent Therkelsen**, Product Manager, Bureau of Criminal Apprehension, St. Paul, Minnesota

Among jurisdictions that have implemented eWarrants and eWarrant systems, the benefits of doing so have far outweighed any concerns about the impact on officers and courts for having to obtain warrants for all DUI blood tests. In particular, use of eWarrants and eWarrant systems can significantly streamline the arrest process, allowing officers to complete requests in their patrol cars on tablets, smartphones, or computers. This practice reduces the amount of time that officers are off the street and the amount of time between the request, approval, and execution of the warrant. Use of an eWarrant system, in which electronic transmission of the warrant affidavit and judicial approval are done through an online information management system, further streamlines the process.

Although efficiency is one of the more obvious benefits to the use of eWarrants, other important benefits exist with regard to caseload and workload. Members of an expert working group noted that the use of eWarrants has resulted in fewer continuances, which in turn reduce the amount of overtime pay to law enforcement officers who are often required to appear at court each time a case is reset. Prosecutors in the working group cited reduced workload due to being able to access warrants electronically. In addition, having the BAC test results leads to faster plea deals, fewer trials, and faster case processing times overall.

The automated nature of the content of most eWarrants also results in fewer mistakes and errors in the request, which in turn means fewer warrants are rejected by judges. As such, there is a greater likelihood that a blood test will be obtained, resulting in better case outcomes and more appropriate sentencing. Moreover, eWarrants can help reduce liability for wrongful arrest or wrongful conviction allegations.

In addition, there are economic benefits to higher conviction rates as well. Members of the expert working group confirm that there has been an increase in the fines and fees revenue generated from DUI convictions since the implementation of eWarrants.

Finally, eWarrant systems produce a number of other less obvious benefits that are more process-oriented. Among these, working group members cited:

- Increased security as a result of authentication protocols for system use, signature, and transmission;
- Ability to track, in real time, warrant status; and,
- Ability to track performance metrics such as average processing time from submission to approval and the common reasons for why judges reject warrants which can be used to inform and improve law enforcement training.

INTRODUCTION TO THE GUIDE

This implementation guide is intended to offer guidance to law enforcement, prosecutors, court administrators, judges, and policymakers on the design/implementation or refinement of eWarrant systems. Built from case studies of eWarrant systems and with input from law enforcement, prosecutors, and judges, as well as an expert working group panel, the guide offers insight for practitioners on a range of systems—from simple, locally-based examples to sophisticated and integrated statewide systems. The end result is an array of options that can be implemented by agencies of varying size, resource levels, and technological capacity.

Development of the Guide

In late 2016, the Foundation for Advancing Alcohol Responsibility (Responsibility.org) awarded a grant to the Justice Management Institute (JMI) to create a best practices guide for implementing and using eWarrant systems. JMI conducted a multi-phase study to document effective eWarrant systems.

Phase one JMI focused on identifying legislative mandates and statutes governing the use of technology applications for search warrants. A legislative scan was conducted to identify which states permit the use of electronic warrants for searches and/or the establishment of probable cause. Once the states were identified, JMI did comparative analysis of other legislative reviews conducted by organizations such as the National District Attorneys Association's (NDAA) [National Traffic Law Center](#) (NTLC) and conducted a content analysis of statutory language. The content analysis resulted in the identification of common themes and key legislative elements related to the following:

- Types of cases for which eWarrant use is permissible;
- The electronic mediums that are permissible (e.g., fax, email, video/telephone conference, text messages, etc.);
- Requirements related to oaths and allowance of electronic swearing in of officers; and,
- Allowance of electronic or digital signatures.

The findings from the legislative review served as the foundation for the second phase of the study, which was focused on gathering information from practitioner groups.

Phase two JMI conducted a series of web-based focus groups to discuss critical issues related to the implementation and use of eWarrant systems. Focus groups were conducted with prosecutors and judges. A focus group was also planned with defense attorneys, but because of the small number of defense attorneys who were able to participate, JMI conducted one-on-one interviews with two attorneys. JMI also conducted interviews with law enforcement officials around the country. Focus group participants included individuals from jurisdictions of varying size and geographic location. During each 90-minute web-based meeting, focus group participants were asked to discuss the pros and cons of different types of systems, logistical considerations related to the implementation and use of eWarrants, legal concerns and considerations, and factors affecting timeliness and accessibility. Participants were also asked to identify criteria for what constitutes best practice, as well as any jurisdictions that they used to model their systems after or that they felt represented best practice.

Phase three JMI used the results from the legislative review and the focus groups to select five jurisdictions for intensive case study. Jurisdictions were selected in consultation with Responsibility.org based on the type of eWarrant system, as well as diversity in geographic location, court structure, jurisdiction size, and legislative framework supporting the use of eWarrants. The five jurisdictions selected were diverse in terms of their systems ranging from locally-based systems to integrated statewide systems.

- Arizona (Maricopa County)
- Delaware
- Minnesota
- Texas (Montgomery and Lubbock County)
- Utah

In-depth interviews were conducted with individuals involved in the design and implementation of the eWarrant systems to document the following:

- Planning and design process;
- System funding;
- Technology platforms utilized;
- Implementation challenges; and,
- Overall system effectiveness.

The case study interviews were compiled into reports describing the systems (included in [Section 7](#)) and analyzed to identify common themes and patterns across the sites that emerged as best practices.

Phase four The final phase of the study was designed to obtain input from experts in law enforcement, prosecution, court administration, the judiciary, and policy on the findings from the legislative review, focus groups, and case studies (See [Appendix A](#) for a list of working group panel members). JMI convened the expert working group for a day and a half meeting to discuss the themes identified in the case studies and to obtain their perspective about the most effective strategies for designing and implementing eWarrant systems, funding and resource allocation, and overcoming common challenges. In addition, the expert working group offered insight on critical legislative language and recommendations for furthering the ability of law enforcement, prosecutors, and judges to effectively respond to DUI.

The resulting product from these phases was the development of this implementation guide for practitioners. Expert working group members and representatives from the case study jurisdictions reviewed the final guide and offered their own testimonials about their experiences with eWarrants.

Guide Components

The guide is designed to provide detailed information for practitioners and policymakers on the fundamental issues about how to get started in creating an eWarrant system, ongoing system operation and maintenance, and planning for unintended consequences associated with the use of eWarrants. The guidance provided is based on best practices from around the country and should be viewed as a menu of options that are intended to be scalable as agencies vary in their size, access to resources, and technological capacity.

The guide components include the following:

- **Legislative framework:** provides a summary of current statutes and insight into key legislative components that can support the implementation and use of effective eWarrant systems.
- **Planning and designing:** provides a discussion of the planning processes to be undertaken in designing an eWarrant system. Specifically, information is provided on engaging stakeholders in a collaborative process, conducting analyses, identifying technological requirements, and managing change.
- **Funding:** explores different funding methods that have been used to cover system design, implementation, and maintenance costs.
- **Policy and operation:** discusses operational policies that jurisdictions should consider prior to full implementation of an eWarrant system.
- **Measuring effectiveness:** describes the types of metrics that should be built into the eWarrant system or documented to provide insight on how well the system is operating, usage, and overall impact on a jurisdiction's ability to successfully investigate and prosecute DUI offenses.
- **Case studies:** provides a detailed overview of the eWarrants and eWarrant systems being used in the jurisdictions studied by JMI.
- **Troubleshooting and mitigating unintended consequences:** discusses different challenges that may arise and negative impacts that can be produced unintentionally, along with strategies for addressing both.
- **Best practices and lessons learned:** summarizes the best practices and key lessons learned from JMI's study and the experiences of those jurisdictions that have implemented eWarrant systems.

Implementation resources, including sample templates, language, and system schematics, are included in the Appendices.

¹ Driving under the influence (DUI) is the abbreviation most commonly used to encompass impaired driving offenses. For the purpose of this report, DUI is the most frequently used term to describe drunk driving. Other abbreviations (e.g., DWI, OUI, OWI, etc.) may appear when discussing laws specific to the states where case studies were conducted.

² The definition of a hardcore drunk driver, taken from the Foundation for Advancing Alcohol Responsibility's National Hardcore Drunk Driving Project, is "[an individual] who drives with a high BAC of .15 percent or above, or who drives repeatedly with a .08 percent or greater BAC, as demonstrated by having more than one impaired driving arrest, and is highly resistant to changing [his/her] behavior despite previous sanctions, treatment, or education."



IMPROVING DUI SYSTEM EFFICIENCY

A Guide to Implementing Electronic Warrants

SECTION 2

Legislative Framework

SECTION 2: Legislative Framework

The Fourth Amendment of the U.S. Constitution grants rights to every American citizen “to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures” and that probable cause must exist for the issuance of a warrant. All 50 states have legislation governing search and seizure that define probable cause, exceptions to the search warrant requirement, and unique restrictions such as the timeframe for the execution of a warrant or rights if a warrantless search is conducted.

In reviewing state legislation, JMI found that 45 states include language allowing the issuance of warrants based on telephonic, video, or electronic affidavits. [Appendix B](#) contains a matrix of state rules, statutes, and operative language.¹ However, as discussed later in this section, although legislation is recommended because it creates consistency, it is not necessary.

SUMMARY OF LEGISLATION

The allowance of eWarrants is codified in a number of different ways. As shown in Table 1, there are 26 states and the District of Columbia that have specific legislation governing the issuance of eWarrants; 8 states in which court rules address eWarrants, and 11 states in which it is a combination of legislation and court rules. Notably, Delaware, Connecticut, Massachusetts, Mississippi, Rhode Island, and West Virginia have no legislation or court rule/order governing eWarrants.²

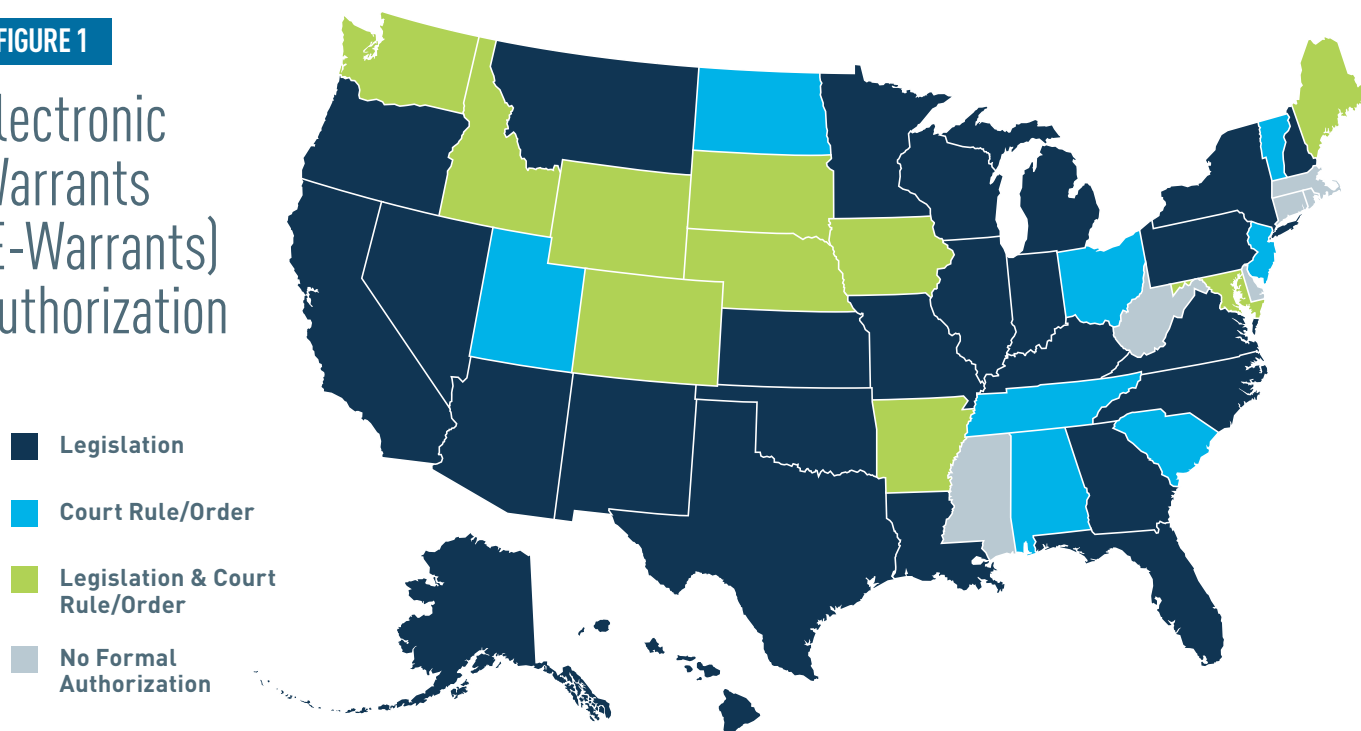


Table 1: State Legislation and Court Rule/Order Authorizing or Governing the Use of eWarrants

State	Legislation	Court Rule/Order	Both Legislation & Court Rule/Order
Alabama		●	
Alaska	●		
Arizona	●		
Arkansas			●
California	●		
Colorado			●
Connecticut			
Delaware			
District of Columbia	●		
Florida	●		
Georgia	●		
Hawaii	●		
Idaho			●
Illinois	●		
Indiana	●		
Iowa			●
Kansas	●		
Kentucky	●		
Louisiana	●		
Maine			●
Maryland			●
Massachusetts			
Michigan	●		
Minnesota	●		
Mississippi			
Missouri	●		
Montana	●		
Nebraska			●
Nevada	●		
New Hampshire	●		
New Jersey		●	
New Mexico	●		
New York	●		
North Carolina	●		
North Dakota		●	
Ohio		●	
Oklahoma	●		
Oregon	●		
Pennsylvania	●		
Rhode Island			
South Carolina		●	
South Dakota			●
Tennessee		●	
Texas	●		
Utah		●	
Vermont		●	
Virginia	●		
Washington			●
West Virginia			
Wisconsin	●		
Wyoming			●

FIGURE 1

Electronic Warrants (E-Warrants) Authorization



*As new legislation or court orders are introduced, this [map](#) will be continually updated.

Despite the variation in how eWarrants may be codified, there are a number of common themes that emerge from an examination of the legislative and court language. These themes include transmission mechanisms, sworn testimony, and signatures.

Transmission mechanisms refers to the specific methods defined in the legislation by which warrants can be transmitted, and include facsimile, videoconference, telephone, and e-mail.

Twenty-two states have language and/or court rules that allow transmission of the warrant electronically either by facsimile or other electronic means (Alabama, Alaska, Arizona, Arkansas, California, Colorado, DC, Idaho, Illinois, Indiana, Louisiana, Maryland, Michigan, Minnesota, Missouri, Nebraska, New Mexico, Oregon, South Carolina, Tennessee, Vermont, and Virginia).

The degree of specificity varies, for example:

- North Carolina's statute reads "written affidavit or 'oral testimony under oath by means of an audio and video transmission in which both parties can see and hear each other'" — N.C.Gen.Stat. §15A-245
- Wyoming's statute reads "all communication between the judicial officer and the peace officer or prosecuting attorney requesting the warrant may be remotely transmitted by voice, image, text or any combination thereof, or by other means and shall be recorded. The testimony and content of the warrant shall be recorded by writing or mechanical, magnetic, electronic, photographic storage or by other means." — W.S. 31-6-102(d)
- Georgia's statute, on the other hand, is more detailed, and reads "search warrants may be issued 'by video conference' provided that when a judge issues such a warrant, the judge is physically located in the state; the judge shall administer an oath to any person testifying; a video recording shall be submitted and maintained as part of the record, and the judge and the affiant shall sign their respective documents 'by any reasonable means' by which they can be identified, including, but not limited to a 'typewritten name, signature affixed by electronic stylus, or any other reasonable means'" — O.C.G.A. §17-5-21.1

Sworn testimony provides the requirements for how oaths are to be administered and whether such oaths need to be administered in person or by some other electronic means.

- Alaska, Georgia, Illinois, Maryland, New Mexico, and North Carolina include specific language that allows testimony electronically via telephone, video, or audio video transmission.
- Maryland includes “in-person,” leaving the potential open for judges to require in-person testimony.
- New Mexico’s legislation also allows judicial discretion for testimony, stating that the judge “may require appearance ‘personally, telephonically, or by audio-video transmission.’”
- A number of states, such as California, Florida, Kansas, and Montana,³ also have separate penalty of perjury statutes that allow for written sworn declaration to the facts that eliminates the oath requirement.

Digital signature provides guidance on how officers and judicial officers can sign the affidavit and can include original signature, typewritten names, and signatures affixed by an electronic stylus.

Fourteen states address digital signatures explicitly (Arizona, California, Colorado, Florida, Georgia, Hawaii, Indiana, Louisiana, Michigan, Montana, New Hampshire, New Mexico, Tennessee, and Washington).

The language on digital signatures varies widely, for example:

- California’s legislation reads “...affiant’s signature (which may be original, digital, or electronic)” — Cal Pen Code §1526
- New Mexico’s legislation reads “...signatures may be by original signature, by copy of an original signature, by a computer-generated signature or ‘any other signature otherwise authorized by law’.” — 5-211 NMRA
- Montana’s legislation is more prescriptive and reads “the judge may administer an oath or affirmation by telephone, and the testimony must be subscribed to the applicant and ‘attached to or logically associated with’ the applicant’s electronic signature; a recording must be made by either the judge or the officer, and in either case, it must be transcribed verbatim as soon as possible; if

the warrant is approved over the phone, the officer shall sign the warrant in the officer’s name and in the name of the judge, and if the judge signs the warrant by electronic signature, the peace officer must initial the judge’s signature and the officer’s signature ‘to indicate that the signatures were made electronically in accordance with this section’.” —46-5-222, MCA

CRITICAL LEGISLATIVE ELEMENTS FOR SUCCESSFUL IMPLEMENTATION

Clearly there is variation in the statutory language and elements included across the states that have statutes or rules governing eWarrants. Although not all states have legislation on eWarrants (as in the case of Delaware), statutes and/or court rules are recommended as they provide standards and uniformity in practice, which help to guard against legal challenges.

If a state is considering the passage of legislation or amending current legislation, there are certain elements deemed to be critical (refer to the following subsection for a model legislation checklist). In terms of key language, experts recommended that legislation and court rules/orders facilitate a streamlined process and align the process with available technologies. Specifically, allowing the transmission of a warrant via facsimile or other electronic mechanism, but still requiring in-person testimony, reduces the timeliness for issuing the warrant, which is critical given dissipation rates of alcohol and other controlled substances. A preferred approach, as noted by many experts at the working group meeting and in focus groups, is to allow officers to sign a penalty of perjury statement or to swear to the testimony via telephone or audio-visual transmission. This helps to eliminate the time needed to appear in person before a judicial officer or magistrate and ensures a streamlined process.

In addition to the officer’s oath, the mechanism by which signatures are affixed to the officer’s sworn affidavit, as well as the judge’s signature on the warrant is important. Allowing digital signatures, whether they are done by electronic stylus or using certified digital signatures generated by computer, is seen by experts as the most efficient way to process warrant requests.

To help ensure that eWarrants are effectively implemented and used, experts also pointed to several areas in which legislative language or court orders could be improved. In particular, the expert working group recommended:

- Language criminalizing the refusal to submit to testing authorized by a warrant.
- Reporting of test results above the legal limit to state driver licensing agencies (e.g., department of motor vehicles).
- Incorporation of an authentication component to verify eWarrant system users' identity, which would help address issues related to in-person testimony.
- Language that addresses an option for recording the oral statement of the officer, certification by the judge that the recording of the sworn oral statement is a true recording under oath, and the retention of the recording as part of the record of proceedings.

Finally, the expert working group members cautioned against certain legislative elements. In particular, the group felt that legislation should not include language related to the return of service, noting that in their experience, it was preferable to let local jurisdictions adopt practices that will be most effective for their locality. There were also concerns expressed about the issue of retention, particularly for video, and the potential impact on an agency with regard to Freedom of Information Act (FOIA) requests. As such, any language in court rules/order or legislation should take into account how retention requirements might impact existing resources.

Perhaps above all else, legislative language should not be overly prescriptive. Those who have implemented eWarrant systems note the need for flexibility that allows for advances in technology and for modifications that will ensure maximum efficiency and effectiveness for officers seeking warrants.

MODEL LEGISLATION CHECKLIST

Based on the statutory review, interviews with practitioners and policymakers, and case studies of jurisdictions that have implemented eWarrants and eWarrant systems, the following checklist enumerates the legislative elements deemed to be the most critical for supporting effective and efficient systems. The actual elements that are desirable in a specific state or jurisdiction will vary based on the type of system used.

- ✓ Provision for the transmission of the warrant by electronic means, ideally allowing for flexibility to adapt to emerging technologies by not prescribing the specific electronic or digital methods of transmission.
- ✓ Provision for oral testimony by telephone or video to allow officers to be sworn in remotely without having to give the oath in-person.
- ✓ Language that addresses the need for recording the oral statement and certification by the judge that the sworn oral statement is a true recording under oath.
- ✓ Language that addresses the retention of the recording as part of the record of proceedings.
- ✓ Inclusion of sworn statement under penalty of perjury to provide further efficiency (i.e., allowing the officer to electronically sign a penalty of perjury statement in lieu of providing testimony).
- ✓ Permission for electronic or digital signature by the officer and the approving judge, judicial officer, or magistrate, ideally allowing for flexibility for emerging technologies, but at a minimum including electronic encrypted digital signatures, signatures affixed by electronic stylus, or typewritten signatures.
- ✓ If electronic or digital signatures are going to be permissible, inclusion of language related to identity verification protocols should be included, again without being too prescriptive to allow for flexibility as security protocols evolve.
- ✓ Language allowing the reporting of failed tests to licensing agencies, ideally allowing for electronic information exchange between eWarrant systems and licensing agency systems.

¹ The legislative summary includes findings from JMI's legislative review as well as a summary compiled by the National District Attorneys Association's National Traffic Law Center.

² The lack of legislation or court order does not necessarily mean that eWarrants are not permissible, but rather that there is no explicit reference to the use of electronic means for transmission. The statute in the State of Delaware, for example, simply states that a warrant application must be in writing and signed, but does not specify requirements for the transmission or return of warrants.

³ See CCP § 2015.5; Fla. Stat. 92.525; K.S.A. 53-601; and MCA 1-6-105.

IMPROVING DUI SYSTEM EFFICIENCY

**A Guide to Implementing
Electronic Warrants**

SECTION 3

**Planning & Designing
an Electronic
Warrant System**

SECTION 3:

Planning & Designing an Electronic Warrant System

Time needed for high-level preparation is predicated on the capacity of the jurisdiction to build institutional support, assemble a collaborative project management team, and secure funding. This may take up to six months or longer, with additional time necessary for procurement if a consultant is sought to assist with the business process analysis. Nonetheless, the major steps to planning and designing an eWarrant system include:

- Identifying and engaging agencies and individuals to be involved.
- Engaging in high-level preparation.
- Analyzing business processes.
- Determining technological requirements.

Each of these steps is discussed in detail below.

STAKEHOLDER ENGAGEMENT AND THE COLLABORATIVE PROJECT MANAGEMENT TEAM

Among the greatest lessons learned from jurisdictions that have implemented electronic warrant systems is the need for robust planning in the design phase. Central to the planning process is collaboration to help align multiple perspectives with legal issues, processes, and technology. Effective eWarrant systems require input from a variety of stakeholders, both traditional and non-traditional. In each of the jurisdictions studied by JMI, a premium was placed on early collaboration—involving judges, law enforcement, prosecutors, and information technology personnel at the state or county levels—as part of the project management team. There are other individuals though who can provide useful insight on the design of the system and its implementation, including legislators, laboratory technicians involved in the analysis of blood tests, the defense bar, county or state government representatives for the procurement process, state department of transportation/office of highway, traffic safety resource prosecutors (TSRPs), sheriffs and police chief associations, and the state driver licensing authority to name a few.



Tips for Creating Effective Collaboration

“To have an effective e-Warrant system, you must have the right team because independently, no single person or agency can solve the issues that arise when you’re creating a new system. Using an existing collaborative body, such as an impaired driving council or traffic records committee can serve as a great starting place as many of the necessary people are already at the table.

It can’t just be anyone though—you need to have the right people at the table and the right people leading and facilitating the work. Members of the team should be executive level decision-makers or their designees, who have the authority to enter into agreements on behalf of their agency.

The person responsible for leading and facilitating the work should be someone with institutional knowledge of the criminal justice system, knowledge about how systems work generally, and knowledge about who the right people are to talk to, or at least how to find the right people. Beyond this, the leader should be organized, inquisitive, outgoing, and able to keep the work moving forward.”

—Darrin Grondel, Director, Washington Traffic Safety Commission, Olympia, Washington



There are two primary steps that should be taken to engage stakeholders and to build a collaborative project team:

1. Identify the appropriate stakeholder groups
2. Create a system to solicit their input and foster participation in planning

These steps should be undertaken first, before any planning or design of the system commences.

Step 1: Identify Stakeholders

In deciding which agencies or individuals should be engaged during the planning process, it is important to consider which agencies will have a role or will be impacted by the implementation of eWarrants. Key questions to consider in making this decision include:

- Who will be responsible for funding or identifying funding sources for the implementation and ongoing maintenance of the system?
- Which agencies' budgets or resources may be impacted by the implementation of eWarrants? (e.g., will the courts need additional personnel? Does law enforcement have hardware that allows them to connect to a system remotely?)
- What are the legal issues related to the eWarrant process, and who is likely to address these at a statutory level and a local level?
- Are there local court rules or other local practices that will impact the design of the eWarrant system?
- Who can provide input on what the technological needs will be for implementing an eWarrant system?
- Which agencies or individuals will have a role in the actual programming of the system or defining the technical requirements for procurement?
- Which individuals/agencies might be likely to challenge the design or implementation of the system?

Ultimately, the identification and inclusion of stakeholders should be based on assessments of who has a vested interest in the eWarrant process, the system design, and day-to-day use. In addition to these considerations, consistency in practice will be important as eWarrants are implemented. As such, thought should be given to how such consistency will be built into the process. If the design and planning is occurring at

the state level, engagement of local justice practitioners (law enforcement, prosecutors, judges, etc.) should be considered, particularly if local rule will determine how the state system will be used locally. Likewise, if planning is occurring at the local level, it will be important to include certain state level representation in the process – notably those who may provide funding or can offer insight from other parts of the state such as TSRPs or state sheriff/police chief associations.

Step 2: Create a Plan for Soliciting Input

Once the key stakeholder groups have been identified, it is important to create a plan for soliciting their input. First and foremost, the plan should articulate specifically what the focus of the collaboration will be (i.e., to design and implement an eWarrant system). Next, the plan should provide meaningful opportunities for people to provide input and feedback throughout the planning process. Specifically, the plan should include a clear calendar of milestone dates, including any in-person meeting dates and times, telephone or videoconference meetings, and critical dates for deadlines related to the planning process. In addition, the plan should specify expectations for stakeholder involvement and articulate what is being asked of them from a contribution standpoint.

As part of developing the input plan, consideration should be given to how different perspectives will be incorporated in the process:

- Will input be needed solely from agency heads and decision-makers, or is it necessary to engage frontline personnel and individuals who will be using the eWarrant system on a daily basis?

TIP

To implement any new system or alter the status quo it is imperative to obtain buy-in from key stakeholders.

Fostering acceptance for and managing change is an integral component in both the development and implementation phases of transitioning from a paper-based to an electronic warrant system.

- Does the agency have people in information technology positions who would be able to provide additional ideas about using existing resources or integration with other platforms?
- Does that agency have an in-house legal department that would need to review any policies or practices envisioned as part of the eWarrant system?
- Who handles budgeting and planning for the agency? If there is going to be cost-sharing among several entities, is their input important? How will they be involved?

Structured engagement is recommended, meaning that stakeholders should understand the decision-making process and what their role in that process will be. Not all stakeholders necessarily need to be involved in every decision. The plan should articulate which individuals or agencies will make final decisions, if there will be an executive committee, or if all involved will have a “vote.” In addition, the plan should also demonstrate to all stakeholders engaged in the process how progress will be measured and what they can expect in terms of feedback on the progress.

The plan should also name the collaborative management team that will be responsible for carrying out the actual planning tasks. These tasks include high-level preparation, business process analysis, and analysis of technical requirements, which are discussed later in this section.

Change Management

A significant part of designing and implementing a new system is being able to manage change. There are four primary steps to change management:

- Active listening
- Identifying organizational priorities
- Addressing uncertainty
- Continuous improvement

Active listening is an important component of stakeholder engagement. It requires giving full attention to what is being said and understanding what stakeholders are saying without offering judgement or opinion. Essentially, this is the opportunity to let people be heard. Active listening requires that the “listener” remember specifically what was said and to respond in a way that demonstrates understanding.

The second step is identifying organizational priorities and is part of active listening. Resistance to change often stems from a lack of understanding about a stakeholder’s priorities – both strategic and universal. In the context of DUI and eWarrants, strategic priorities are external to the organization or agency and are focused on the individuals who come into contact with law enforcement or into the courts for DUI offenses, as well as the general public. For law enforcement, these priorities are likely to focus on guarding against wrongful arrest or police mistreatment of suspects as well as the public’s perception of safety as it relates to impaired driving enforcement.

Universal priorities, on the other hand, are those priorities that are important to the organization or agency for its day-to-day operations, and are largely employee or workload focused. The implementation of eWarrants is likely to have a significant impact on law enforcement and prosecutors’ universal priorities because they have the potential to streamline processes, reducing the time needed for making the arrest, and resulting in stronger evidence to build cases. For the judiciary, the universal priorities may be more focused on how they will staff and respond to warrant requests 24 hours a day, 7 days a week.

The third step to managing change is being able to identify and address uncertainty. In general, there are four types of uncertainty that need to be considered:

- **Variation:** uncertainty that comes from plans that do not necessarily align with what is realistic, practical, and feasible.
- **Foreseen:** identifiable and predictable influences such as the need to connect to older legacy systems that may require system updates.
- **Unforeseen:** influences that cannot be predicted (e.g., technology failures, sudden changes in key leadership positions in stakeholder agencies, or legislative changes impacting the types of permissible electronic transmission methods).
- **Chaos:** stems from the structure of the plan itself when all or parts of the plan are uncertain with no actionable backup plans.

Stakeholders should work together to identify which of the uncertainties may arise in the implementation of eWarrants. Once identified, it is critical to develop alternative steps, measures, and contingency plans to address these potential uncertainties.

The last step in change management is continuous improvement. Virtually every implementation effort encounters barriers and challenges along the way. Staying focused on identifying and addressing these challenges in a way that promotes continuous improvement will build stakeholder trust and ensure that the implementation of an eWarrant system does not fail.

High Level Preparation

Once a collaborative project management team has been identified, a deliberate planning process should be followed, starting first with a series of high-level preparation tasks as follows:

1. Clearly state the problem to be solved

First, the team must articulate what issues the system will address. This should be framed in terms that are as specific and targeted as possible. Examples of problem statements for an eWarrant system include the following:

- “The eWarrant system will be built for a ‘four-county region in the Seventh Judicial Circuit of [State], to be used by participating law enforcement agencies seeking warrants from the Magistrate and Circuit Courts.”
- “Currently, the time for review and issuance of approved search warrants requires a personal appearance by a law enforcement officer and may take up to 24 hours. This directly impacts the utility of warrants for time-sensitive searches, including for blood draws to test for blood alcohol levels of impaired driving suspects.”
- “The intent of the system is to reduce the time for review and issuance of approved search warrants for standard affidavits to less than two hours and ensure that suspects’ Fourth Amendment rights are not violated.”

In addition to the problem statement, agencies should clearly define the goals and objectives of the eWarrant project. Some examples include the following:

- Automate the process of seeking a search warrant from a judge, based on probable cause.

- Consider the use of video, audio, digital affidavits, or other technologies available that will provide for the most effective and efficient eWarrant system.
- Simple search warrant requests should be able to be conducted from an officer’s vehicle; more complex search warrant requests should be able to be conducted from the precinct station, without going to the courthouse.

2. Decide on a high-level approach

Initially, there will be several key, up-front decisions to be made by the project management team. It is recommended that these issues be considered and addressed before moving forward with system development.

First, determine who will conduct an analysis of the current process for requesting and issuing warrants (i.e., the business process analysis). The team should identify whether this analysis can be conducted in-house or whether a contractor/consultant must be hired. If the latter is required, this will have budget implications.

Second, identify who will be the lead organization to manage the analysis. For an eWarrant system, the logical organization might be the courts, with law enforcement as a close partner. Often law enforcement is comprised of multiple agencies (e.g., state police/highway patrol, sheriff’s departments, local police departments, and university police departments to name a few). However, in a number of jurisdictions JMI studied, the lead organization was the agency that managed the state criminal justice information system and records.

Next, determine whether an existing system already has a built-in solution by considering the following:

- Does law enforcement already have an eWarrants module or add-on associated with their field reporting system (if they have one)?
- Do the courts have e-charging, e-discovery, or other electronic systems in place?
- Does the court case management system already have an eWarrants module or add-on?
- Is there a local or state criminal justice information system that has document management modules or can support an eWarrant application?

If none of the above appear to be a potential solution and eWarrants cannot be added to an existing system, no more than two or three basic approaches should be considered, even if not resolved at this phase. For the creation of a standalone eWarrant system, options to consider should include:

- Customized-off-the-shelf (COTS) software like the document management software used in Texas (see case study on Texas for more information) or software as a service (SAAS – totally contracted service) solution in which a vendor is hired to create a system from the ground up (see [Appendix D: Sample RFP from Washington State Patrol](#)), remembering that a SAAS model should mandate very specific agreements over data, documents, and records.
- Public Internet; proprietary network (Intranet); or closed circuit (usually licensed) communications.

Finally, one agency/entity must be designated with the authority and responsibility to address future issues as they arise. The project management team should identify which agency is best positioned to pay for ongoing maintenance, licenses, and fees for security and patches. This may not be able to be determined until later in the budgeting process.

3. Know your budget

While budgets are subject to change over the course of a project, it is highly recommended that a high-level estimate of costs, using information from other jurisdictions, and possible blind consultation with vendors and consultants be developed early in the planning process. Based on the experiences of agencies contacted for this review, it is further recommended that a contingency of at least 15% be added to the budget at this early phase. Although costs will vary widely depending on the scope of the effort, cost estimates may be as low as a few thousand dollars for equipment (as in Montgomery County, Texas) or several hundred thousand dollars (for Minnesota to build eWarrants into an existing e-Charging system).

The project management team is also encouraged to identify possible funding streams and resources as early in the process as possible (see [Section 4](#) for more information about potential funding sources). Generally, technology acquisition for eWarrants might have shared costs. This is a critical moment. When [Pennsylvania built an eWarrants system](#), the courts supported most of the development costs, but then assessed fees to local counties and law enforcement agencies to implement the system across the state. Not all counties and law enforcement agencies chose to participate as a result.

4. Map a planning process in terms of time, resources, and responsible parties

An initial planning process should be done regardless of whether the business process analysis is being done in-house, or by a consultant/subject matter expert. This should follow a standard analysis process, for which there are many variations. Most methodologies will follow a variant of the seven steps described in the following section.

Teams are encouraged to name the project management team on the client side, even if the analysis is being done by a consultant. They will be responsible for communications, coordination of site visits and meetings, adherence to budgets, and many other responsibilities.

5. Procure technical assistance

If using in-house business process analysis, this step is not required. If using a consultant, agencies will need to bid out the technical assistance.

Business Process Analysis

Business process analysis is a proven technique for clearly defining needs and solutions to those needs. For an eWarrant system, the analysis will necessarily deal with software, hardware, and processes. The business analysis will typically take between six to nine months, again depending on the local technology infrastructure and the capacity of each stakeholder to plan for new technologies. Other key factors include the amount of existing documentation of processes and procedures, forms and reports, and host systems. The following steps are commonly used in a business process analysis, tailored to an eWarrant system. The deliverable is often called a business requirements document (BRD), which provides specific details about the solutions that will be implemented for the eWarrant system.

1. Undertake information-gathering

To begin the business analysis, it is important to first gather all information relevant to the existing processes. This includes the following, all of which should be formal and structured, but also continuous throughout the process:

- Data collection and gathering of existing process documentation.
- Interviews and site visits to gather requirements from key stakeholders and users.
- Statutory research.

2. Map the existing “as-is” business processes

In order to work towards change, it is necessary to understand the processes that are already in place. Using the information gathered, analysts can map the existing business processes in the following manner:

- Narrative description.
- Workflow diagrams (e.g. swim lane, layered event model, decision model).¹
- User lists.
- Data and document index and repository.

3. Map the new, proposed business processes

To identify what the new processes will entail, the following components should be completed:

- **Business requirements document (BRD):** details the needs and goals related to the eWarrant system, the processes required to meet these needs/goals, the factors that will influence what is built and why, and documentation of user needs and expectations. A sample is included in [Appendix C](#).
- **Requirements traceability matrix (RTM):** links the business requirements in the BRD throughout a validation process that tests all the requirements of the system.
- **Workflow diagrams:** graphically illustrate the key decision points, how a warrant will be processed under the new system, and the “touchpoints” at which individuals will engage with the system (e.g., logging in to the system to initiate a new warrant request, retrieving a request for approval, recalling a request to make corrections, etc.).² Note that these diagrams should vary considerably from existing processes.
- **Business rules:** state models and guidelines for the system from a user perspective, which generally identify the different branches of choices for each case and how they impact the “state” of a case.
- **User roles and permissions:** specify what information individuals will have access to and permissions for individuals to modify the system.

4. Identify all data and information exchange touchpoints

To complete a comprehensive review of touchpoints, documentation should typically include:

- Index of data or information exchange touchpoints between different systems or parties, usually indexed on the workflow diagrams (see no. 3 above). For example, some of the systems studied by JMI are linked to state criminal history databases from which prior DUI conviction data can be drawn and “uploaded” into the eWarrant system. The index would specify the point in the process where this exchange would occur as well as the specific data that will be accessed.
- Table of documents or data that are exchanged at each touchpoint.
- Rules about data ownership and governing what other parties can do with the data.

5. Catalogue all forms and documents to be automated

Most systems, even paperless, have documents. In an eWarrant system for search warrants to draw blood, an officer may be required to present the warrant to hospital staff or a physician to authorize the procedure. A copy may be required for the offender. Some states may have rules requiring paper affidavits of probable cause or citations or descriptions of the arrest in paper form, such as Oregon. Some judges prefer to see “forms” and “documents,” such as affidavits, in visual hardcopy format (e.g., PDF), even if not required by law. The documentation for this typically includes:

- Document index with references to the workflow map (see no. 3 above), with indicators of the transmission channels the documents must travel and who the users are by user types (not individuals).
- Document samples from existing hardcopies with clear delineations between smart forms (digital representations of hardcopies) and forms that will be converted into data without the need for a hardcopy version.

6. Define administrative tools

To facilitate the development and/or implementation of the new system, it is necessary to identify who requires access and to what degree as well as the particular values or items that need to be included in order to navigate through the system.

Documentation typically includes:

- Table of user types and roles, usually indexed to functional groups (this is not a list of every user in the system, which will be done during development).
- Lists of values, which are preliminary drop-down lists of values that will be used throughout the system and may be user-defined, depending on their uses.

7. Specify performance requirements

Both agency decisionmakers as well as frontline users of the system will have specific expectations for performance of the system as a whole. For a system like eWarrants, they might include:

- Video and/or audio quality (e.g. broadcast, intermittent, bandwidth dependent).
- Light, medium, and heavy transaction response times.
- Report compilation times.
- Maximum peak load user capacity.

By anticipating these expectations, system developers can work to mitigate issues and ensure that the system functions to meet the needs of its users.

A WORD ABOUT DOCUMENT MANAGEMENT SYSTEMS

Document management systems have several advantages and disadvantages over an information management system. While typically less costly, off-the-shelf systems are fairly easy to tailor to specific needs, the major disadvantage is that such systems do not always have reporting capabilities for analyzing such things as the length of time to process a warrant, the number of warrants issued, the number and reason why warrants were rejected, and so on.

[Appendix C: Business Process Analysis Resources](#) includes samples of the BRD, workflow diagrams, requirements traceability matrix, and data and document indices that can be used to conduct the analyses described in this section.

TECHNOLOGY REQUIREMENTS

A business process analysis for an eWarrant system will need to be paralleled or followed by an analysis of the technological requirements, which should include:

- Involvement of state or county information technology (IT) personnel to help understand what technology options are available currently and what may be needed.
- Consideration of security and privacy issues related to any existing platform or a new platform to be developed, in addition to the design features.
- Identification of what expectations law enforcement, prosecutors, and judges have about how the system should operate, particularly in terms of how they will access and use the system (many of the jurisdictions studied by JMI established user groups comprised of law enforcement, prosecutors, judges, and technology personnel, to provide input on language and format).
 - These user groups should continue to meet after implementation to discuss possible system modifications, enhancements, or challenges.

The jurisdictions studied by JMI used a variety of technologies as the foundation for their eWarrant systems. Utah and Delaware, for example, incorporated the electronic warrant into existing statewide information management systems. On the other hand, Minnesota built its own system in-house, while a jurisdiction in Texas used an off-the-shelf document management software to create its electronic warrants.

Ideally, the eWarrant system can be built onto an existing platform. Beyond the obvious benefit of likely being more cost effective, use of an existing platform can reduce the need for user hardware, benefit from use of existing access and security protocols, and streamline the implementation process. There are, nonetheless, several considerations in building onto an existing platform:

- Does the existing IT environment work well, and if not, are there issues to be addressed that would be impacted by the addition of eWarrants?
- Will the existing network bandwidth support additional volume?
- How will the responsiveness of existing applications and databases be impacted by the addition of eWarrants?
- Do all potential users have access to the existing system? How will that be managed?
- Is there a desire to and/or capability to link the existing system with other systems, such as the department of motor vehicles?
- Is there a need to program data dashboards and reports for tracking data to evaluate the eWarrant process?

Many of these questions are also relevant if a new system will be developed in-house or with off the shelf software. There are a number of other issues, however, that need to be addressed with a new system. For example, is the system simply going to be a document management system that still includes some transfer of paper, or is there a desire for a more robust relational database or information management system? Is there a requirement for the sworn oath to be administered in-person, can it be done by telephone or video conference, or is a penalty of perjury statement and signature permissible? Does the state or county have the in-house capability to create the system or will it be necessary to hire a vendor? If the latter, it will be important to factor in the need for developing the specifications for the request for proposals (RFPs) and what new hardware may be required for implementation. A sample RFP from the Washington State Patrol Information Technology Division to solicit bids for the development of their electronic driving under the influence integration application is included in [Appendix D](#).

Development of technology requirements can be conducted in parallel with a business process analysis, but should be predicated on business requirements. Jurisdictions that engage a consultant often include the development of technology requirements in the scope of work. Key factors include the amount of existing documentation of processes and procedures, forms and reports, and host systems.

Note that some jurisdictions do **not** take this step prior to procurement of a technology solution. Their approach is to publish RFPs that must include a technology solution, inviting creative and alternative ideas, as part of the proposal. For this to be successful, *Step 1: Perform technology information gathering* (below), should be conducted prior to solicitation and included as part of the critically important information provided to the bidders.

The following steps are commonly used in the development of technology requirements, tailored to an eWarrants system:

1. Perform technology information gathering

Similar to business processes, planners should document existing technologies and infrastructure, including:

- Network diagram.
- Network hardware and software, including bandwidth, security, access controls, and operating systems.
- Host systems, if the eWarrant system will be integrated into field or back office reporting systems for law enforcement, or court case management systems (if the eWarrant system is a module of the host system, it is still critical to document other key systems, if integration is required).
- End-user hardware and software, primarily focusing on operating systems, browsers, and any video or audio technology needed.
- Mobile technologies that may be used by law enforcement or other stakeholders.

2. Conduct a technology gap analysis

To ensure that proposed solutions work, a gap analysis is critical. The gap analysis is designed to assess whether the existing network and application technologies will support a solution, or whether the foundational technologies need to be upgraded or supplemented. This step is also crucial to align technology with statutory requirements or constraints. These costs are often missed in planning for new technologies. Tasks include the following:

- **Functional gaps:** if procuring a COTS or SAAS system, the functionality of the new system should be sufficient to meet the detailed business requirements, or at minimum customized in advance. Functionality that must be built later is often much more costly than if it is included in advance. This is the primary purpose of the requirements traceability matrix, which is often used as a foundation for bids by software vendors.
- **Technology integration:** technologies that should be integrated into the eWarrant system and assessed for compatibility are foundational and system-wide for the jurisdiction, court, or law enforcement. These often include document management systems, video and audio conferencing and recording and case management systems. Too often, technology implementations are fragmented and ultimately unsustainable.

3. Define architecture of the new system (i.e., what it is, who owns it?)

Before a system is developed, it is necessary to identify the key components and delineate which agencies or entities have ownership of each of these components. The documentation for this step includes:

- Proposed network diagram.
- Proposed hardware and software specifications.
- Clearly delineated ownership matrix of all system components.
- Data ownership and maintenance agreements between stakeholders.

4. Define suite of technologies that will meet the needs for the eWarrant system

Not every system will require a complete overhaul of technology. To facilitate the planning process and to acquire a better cost estimate for the system agencies should define the technologies needed for the system envisioned. This step must be directly aligned with state statutes, jurisdiction requirements, and acceptable protocols for the courts and agencies. For example, if the jurisdiction is currently using faxed affidavits and warrants, how much will the system simply mirror a document management exchange in digital format?

¹ See [Appendix C](#) for a sample, which is included in the Business Requirements Document Template.

² If the system is designed to interact with other systems (e.g., to access data from the state drivers licensing agency or state criminal history database), the workflow diagram should illustrate the specific points at which the systems will exchange data.



IMPROVING DUI SYSTEM EFFICIENCY

A Guide to Implementing Electronic Warrants

SECTION 4

Funding Electronic Warrant Systems

SECTION 4:

Funding Electronic Warrant Systems

As with any technology solution in criminal justice, the major questions are, “How much is this going to cost, how is it funded, and who is going to pay for it?” There are no easy answers to these questions, and they will undoubtedly vary from state to state, county to county, agency to agency. High-level preparation should provide early cost parameters that will be refined as a result of understanding the technology requirements highlighted in the previous section.

The type of costs will vary – from hardware and software costs to personnel costs for programming. There may also be costs associated with hiring consultants to conduct business process analyses. A good planning process should take all possible costs into consideration to identify opportunities for multiple funding sources and cost-sharing. Among the jurisdictions studied by JMI, costs for design and implementation ranged from zero (in the case of Delaware in which costs were just absorbed as part of the normal function of the Delaware Justice Information System) to \$350,000 in Minnesota to build an eWarrant module into the state’s e-Charging platform.

The jurisdictions studied used a variety of funding sources – including state or grant funding, fees for cost recovery, and other low-cost options – to cover the expense of their eWarrant systems. Agencies that are considering developing their own eWarrant system should explore each of these funding strategies to determine their feasibility.

STATE OR GRANT FUNDING

When electronic warrants are built into existing systems, there is an opportunity to make use of funding that is already provided for state information management systems. In Utah and Delaware, for example, the costs for developing and maintaining the eWarrant system come from the state criminal justice information system funds. Delaware built electronic warrant capabilities into its state criminal justice system at no additional cost to the state, and now receives \$100,000 every five years from the legislature to upgrade equipment for law

TIP

A good planning process should take all possible costs into consideration to identify opportunities for multiple funding sources and cost-sharing.

enforcement to access the system. In Utah, the primary costs not covered by the existing state repository budget were the costs to the courts for phones, laptops, and iPads for accessing the system remotely.

Members of the expert working group convened by JMI reiterated the importance of including representatives from both the agencies that manage state information systems and legislators in the planning phase. In doing so, cost implications and impact on existing resources can be identified early and planned for in upcoming budget requests.

In other jurisdictions, such as Minnesota, eWarrants were built onto the existing e-Charging platform with grant funds from the Department of Public Safety’s Office of Traffic Safety (OTS), which receives funding from the National Highway Traffic Safety Administration (NHTSA). The \$350,000 grant was used to support the business process analysis and quality assurance processes; costs for the actual programming of the system were covered internally (estimated at an additional \$300,000 for labor). In addition, the \$350,000 grant from OTS is renewed annually to cover costs of maintenance and the addition of new features as necessary. In Maricopa County, the Superior Court applied for and received \$30,756 in funding from the Governor’s Office of Highway Safety to cover the costs for the court’s information technology department to create the eWarrant application. An additional \$87,838 was received from the state administrative office of the courts to enhance the application for use by the Department of Public Safety and to hire additional judicial officers and judicial assistants to handle the eWarrant workload.

USE OF FEES FOR COST RECOVERY

In certain jurisdictions, asset forfeiture and other fees levied against offenders are used to recover the costs associated with the implementation and maintenance of eWarrant systems. A DUI fund in Utah was established specifically for cost recovery. Fees paid by offenders are placed in a state interest bearing account. The use of these funds is restricted to requests that focus on alcohol-related crimes, and the eWarrant system is considered an acceptable expenditure. The legislature mandated that impound fees and a DUI surcharge generate monies that are used to maintain their system. The Delaware legislature provides \$250,000 a year to the Delaware Justice Information System agency (DELJIS) for maintenance on the systems from a court assessed fee of \$1.00 on each adjudication of guilty, delinquency, or responsible action. In Illinois, the state allows the use of funds from asset forfeitures to fund private crime labs for blood tests.

LOW COST OPTIONS & ALTERNATIVE FUNDING SOURCES

Jurisdictions that have implemented eWarrant systems note the importance of thinking beyond just funding for the system itself. Hardware (e.g., iPads) has multiple purposes and utility in the criminal justice system. The Supreme Court in Wyoming provided funding for iPads for judges that are used for processing eWarrants as well as for carrying out other judicial responsibilities. The defining of other purposes for hardware, or even software, can produce cost-sharing options to make funding more viable. Finally, other government entities may have a vested interest in the implementation of eWarrant systems. State highway safety offices or departments of transportation are one such source, and in some states, they have been willing to purchase equipment needed for the system such as laptops or iPads.



IMPROVING DUI SYSTEM EFFICIENCY

A Guide to Implementing Electronic Warrants

SECTION 5

Electronic Warrant Systems: Policy and Operations

SECTION 5:

Electronic Warrant Systems: Policy and Operations

A central theme throughout interviews with stakeholders who have implemented eWarrant systems is that consistency ensures reliability and operational policies foster consistency. Although a number of states will have explicit policies enumerated statutorily or through court rule, there are certain key policies that should be considered by jurisdictions seeking to implement or refine electronic warrant systems. These policies focus on authentication and security, officer's oath and swearing to factual statements, and warrant retention. Beyond policy, the expert working group pointed to pilot testing and training as critical elements for ensuring consistency and uniformity in the use of eWarrant systems.

AUTHENTICATION AND SECURITY

Even on a secure system, user authentication is paramount for ensuring that judges can identify the law enforcement officers with whom they are dealing and vice versa. As the process for issuing a warrant moves from paper toward electronic transactions, authentication is a must.

Electronic warrant systems may include both digital documents and the additional need for verbal review and inquiry by a judge. In a digital environment, a telephone call or video conference may easily be set up as part of the communication software. The concern for authentication and security is exacerbated, though, if digital communications occur over public or unsecure networks. Authentication and security risks decrease if the system is both secure and verifiable at each end of the communication and if the network is secure. Authentication and security, then, are categorized on digital systems as user identification and network security.

Why are operational policies so important? These policies foster consistency. For users to have faith in the reliability of a system, there must be consistency.

User identification methods include:

- Login authentication, which authenticates a user before access to the system is granted.
- Network access authentication which authenticates both user identity and application access to the network services.
- IP security authentication which is necessary for officers and judges to electronically sign warrants.

User identification technologies include usernames and passwords, authentication codes, and biometrics. Comparable technologies are used to authenticate electronic signatures by officers on applications and affidavits and by judges on warrants as well as other types of related orders.

Network security, though, is key to determining how secure user identification needs to be. In non-technical terms, if a network is not secure, and access to it is easily compromised, user identification is critical to authentication and security. Network communications between law enforcement and the courts may be provided in a closed network environment, using dedicated, leased lines. But, most network communications today are virtual, or virtual private networks (VPNs), that utilize the public Internet or components of it. Older technologies, such as dial-up connections, are also on the Internet and telecommunications networks that are easily hacked or compromised.

Most network security is provided by server authentication and encryption. Server authentication technologies include, at minimum, secure sockets layer (SSL), first to authenticate the server at the other end and then to provide encryption for all data that is passed across the network. Today, SSL is still widely used, but is being replaced by a more secure protocol, transport layer security (TLS). With TLS, digital certificates are used to identify servers at each end of the communication, with a cryptographic system that uses two keys, public and private. A public key is stored in advance, and a private key is known only to the recipient. Data encryption is key to preventing hackers from gaining access to the servers by intercepting readable data.

In Minnesota, for example, officers and judges are given passwords to access the eWarrant system. They also have the option of a fingerprint login. Delaware uses SSL protocols to authenticate users based on digital certificates. These certificates verify identity before access is granted to the state criminal justice information system, which houses eWarrants. Finally, Utah uses more robust authentication procedures that include receipt of an authentication code through text message, which must be entered before access to the system is granted, a small physical token device that acts as a digital key to the system, or a soft token that is essentially a one-time password that changes every minute.

SECURITY TOKENS

Security tokens contain secret information to prove identity that can include a digital signature, static password, synchronous and asynchronous passwords that are time-based, or biometric data. Although security tokens may seem to be the best option, they are nonetheless susceptible to breach either through the loss or theft of the physical token or if a third party solicits the token information electronically and then submits it to the authentication system.

Decisions about the appropriate protocols should not be made ad hoc. If there are not current authentication and security protocols in place for other systems that can be incorporated into an eWarrant application, jurisdictions should consider conducting a security needs analysis. Such an analysis will help determine:

- What the access rights should be and for whom.
- What information can individuals access and rules for limiting access to select users.
- How data privacy and integrity will be ensured.
- How often security audits will be performed to test for system vulnerabilities.

As noted above, access rights are another element to be considered as part of security. These rights can be articulated through memoranda of understanding as well as more formal interagency agreements. Minnesota, for example, has two legal agreements – the Joint Powers Agreement (JPA) and the Data Sharing Agreement (DSA) – between the state and the governing board (e.g., city council, county board) of the participating law enforcement agency. The JPA defines the scope of the shared data effort and establishes the obligations for each party with regard to use. The DSA is executed to ensure compliance with court rules on the use of system data. The state Bureau of Criminal Apprehension (BCA), which oversees the statewide criminal justice system and electronic applications, requires both of these agreements to be in place before an agency can use an e-Charging (including eWarrants) product.

OFFICER'S OATH

One of the challenges to an eWarrant system is the need to take officers' oaths and have them swear to the facts contained within the warrant. In many places, statute or local rule requires this be done in-person, which can present a barrier to the timely issuance of the warrant. In some jurisdictions, it may be necessary to engage the courts in changing the administrative rules of criminal procedure to allow probable cause statements to be sworn in electronically or digitally as was the case in Utah. In other instances, legislation may need to be changed.

Some of the options identified in the case study jurisdictions and by the expert working group members for addressing oath issues include:

- Adding a penalty of perjury statement on the warrant (i.e., declaring the facts stated in the warrant to be true and correct) which is then signed and dated.
- Allowing the swearing-in to occur over a recorded telephone line or video conference which is permitted in Georgia.
- Allowing law enforcement officers to swear in other law enforcement officers as is common practice in Texas.

RETENTION

The last major policy issue identified by JMI for jurisdictions to consider is that of warrant retention. How long, and where, will pending and executed warrants be retained? In Utah, for example, warrants are available in the UCJIS system for 20 days and can be accessed by authorized users. After 20 days, however, the warrants are transferred to the courts for retention and are no longer available through the eWarrant system. In Minnesota, the retention policy is 60 days from last “touch” and then the warrants are only available through the court file copy. Officers typically file the warrant at the court within 10 days of warrant execution. Delaware, on the other hand, retains warrants indefinitely and the warrants are only removed from the system if the individual’s record is expunged.

In making determinations about the retention policy, some questions to consider include:

- Are there statutory requirements for the retention of records, specifically warrants?
- Which agency will have responsibility for storing the warrants?
- What is the impact on storage space (largely determined by length of retention policies)?
- For what purposes might someone need access to stored warrants, and who would be authorized to access these documents?

Why Pilot Test?

- Determine how the system will function in the real world and a day-to-day basis.
- Identify and address unanticipated problems within the system.
- Make necessary technical corrections.
- Obtain buy-in from frontline users who can champion the benefits of the system among their colleagues.
- Overcome resistance by breeding confidence that the system will function as intended.
- Determine future needs and plan accordingly.

PILOT TESTING


In an effort to identify potential challenges or issues with a new eWarrant system, many jurisdictions have opted to run a pilot test of the system with a subgroup of offenses (some of the jurisdictions studied tested the system on misdemeanor impaired driving) or in a single jurisdiction before going fully “live.” Maricopa County, for example, conducted its pilot test with a single DUI officer from the Phoenix Police Department, and then added others as the pilot progressed. Many of the current statewide systems, such as the one in Utah, began in a single jurisdiction with a single law enforcement agency. The pilot test validates the processes and functionality of the system, identifies potential glitches in the software, and highlights any unforeseen challenges. The pilot test also provides insight into training that will be needed or any areas of additional resistance to change that may need to be addressed.

Although there is no standard timeframe for how long a pilot test should be conducted, it is recommended the pilot test be of sufficient length to:

- Capture a large enough number of warrant requests to test all features of the system.
- Involve several different officers, of varying experience levels, assignment, and geographic locations.
- Test user access on different equipment (i.e., laptop, tablet, smartphone).

Minnesota, for example, conducted a 90-day pilot period, starting with the state patrol only, then adding eight municipal agencies in Hennepin County midway through the pilot.

During and following the pilot test, it will be important to collect and assess feedback. Standardized questionnaires to solicit user feedback, along with metrics on system performance, are both useful tools for systemically documenting the pilot test process. Examples of feedback metrics and questions can be found in Table 2 (note these are intended to be illustrative and not necessarily exhaustive).

 **Table 2: Examples of eWarrant System Feedback Questions and Performance Metrics**

User Feedback	How easy was it to access the eWarrant/eWarrant system?
	How easy was it to navigate through and complete/review the affidavit?
	Were the instructions provided prior to using the system thorough?
	Were any issues encountered that were not covered in the instructions? If yes, what were they?
	What type equipment was used to access the system and prepare/review an eWarrant (e.g., smartphone, laptop in patrol car, tablet, laptop/desktop computer in station)?
	Were any issues encountered during the submission and review of the affidavit? If so, what type?
	Was information about the warrant status accessible?
	Was a notice received about the receipt of a request or the approval/rejection of the warrant?
	What changes to the system should be considered?
System Performance Metrics	Number of times system was accessed
	Average length of time per each access
	Average length of time from transmission to approval/rejection
	Number of failed login attempts

Both user experience and system performance should be analyzed to identify:

- Pervasive issues that may require additional programming or development.
- Aesthetic issues related to layout and format of the online interface.
- Paper documentation that is generated from the system.
- Training needs to provide more clarity for users.

Depending on the scope of revisions identified, particularly those related to reprogramming or development, it may be necessary to conduct additional tests prior to full implementation.

TRAINING

To ensure that users of any eWarrant system are able to navigate the system efficiently, proper training is necessary. The better and more comprehensive the training, the less likely that users will encounter problems, thus minimizing frustration with the process and increasing acceptance and support for the system's use. Important activities for any eWarrant training initiative include:

- Identify all agencies that may require training and education on system implementation and use.
- Identify which entity will be responsible for developing a training curricula and associated materials.
- Identify who will be responsible for conducting training (i.e., will one individual or entity be responsible or will a train-the-trainer format be used?).
- Develop a standard training curricula and materials to be used by all parties involved to ensure consistency.
- Determine when it is most advantageous to train system users and in what venue.
- Explore the possibility of offering continuing legal education (CLE) credits as an incentive for completing the training.
- Update and augment the training to reflect feedback from system users (i.e., as issues with the system are identified, incorporate these into training to educate users on how to troubleshoot effectively or avoid complications).

Findings from the case studies revealed that jurisdictions employ a number of approaches to facilitate the training of practitioners. Some of the most important considerations include identifying the target audience and focus of the training as well as determining how the training will be delivered.

Audience and focus. eWarrant training need not be limited strictly to law enforcement officers. Instead, the audience should be diverse and can include law enforcement, prosecutors, court administrators, court clerks (to the extent they have responsibility for retention), judges, crime lab technicians, and even medical professionals. For individuals working within the justice system, training typically focuses on the reasons for the probable cause warrants for blood draws, how to complete the warrant and use the system, transmission of the requests, and return of service. For crime lab technicians and medical professionals, the training tends to focus on the legal aspects of the warrant process for blood draws.

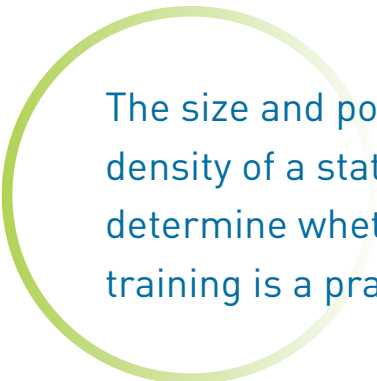
Judicial training is particularly important to acquire the support and buy-in of the judiciary who are integral to the effectiveness of any eWarrant system. In Lubbock, Texas training is delivered to judges on search warrant requirements and the importance of blood evidence in the adjudication of a DUI case. A copy of the training used in Lubbock is available in [Appendix E](#).

Delivery method. eWarrant training can be delivered in-person or electronically and can also be incorporated into law enforcement schools and academies as well as judicial and prosecutor conferences and CLE courses. In most of the jurisdictions studied by JMI, the training was designed to be short and readily accessible to officers, judges, and other users.

In Utah, for example, the eWarrant training was designed to last less than one hour and focused on the changes to the DUI arrest process as a result of the system and the benefits of using the system. The training is offered as an in-person class and as an online course for rural or remote locations. Finally, Utah also includes eWarrant training in its Drug Recognition Expert (DRE) schools (see [Appendix E](#) to view a PowerPoint presentation used with DRE officers).

The size and population density of a state can determine whether in-person training is a practical option. For example, because Minnesota is comprised of many rural counties, the Bureau of Criminal Apprehension's Training and Audio Division opted for an online PowerPoint training that allows officers to complete the training at their leisure and remotely (see [Appendix E](#) to access this PPT). In addition to initial training provided to officers, Minnesota offers a free 24-hour, 7-days per week support line officers can call if questions arise during the arrest process, as well as an online frequently asked questions page. The automated phone system offers assistance with difficulties logging on to the system, editing a DWI event, using breath test equipment, or receiving assistance with suspects in custody. The courts also provide informal training on the system and how to access it.

Regardless of the training approach employed, all jurisdictions should seek to ensure consistency in educational content and materials. Furthermore, it is recommended that feedback be elicited from practitioners to gauge whether the level of information contained in the training is adequate and to determine whether existing materials require updating and/or augmentation. As common issues with system operation and use are identified, training should be modified to make sure that they are addressed.



The size and population density of a state can determine whether in-person training is a practical option.

IMPROVING DUI SYSTEM EFFICIENCY

A Guide to Implementing Electronic Warrants

SECTION 6

Measuring Effectiveness

SECTION 6:

Measuring Effectiveness

Ongoing assessment of eWarrant and eWarrant system effectiveness is critically important for ensuring the intended goals are being met, and if they are not, measures of effectiveness can help pinpoint areas for improvement. There are any number of metrics that can be used to assess usage, user satisfaction, process, and outcomes – many of which should have already been developed as part of a pilot test.

If a jurisdiction is creating an eWarrant system, attention should be given to the types of metrics that can be built into the system as a data dashboard or for regular reporting. These metrics include, but are not limited to, the following:

- Number of system logins (both successful logins and failed logins).
- Number of warrant requests submitted.
- Number of warrants approved and rejected.
- Average length of time from login to warrant transmission.
- Average length of time from retrieval to approval/rejection.
- Average length of time from submission to return of service.
- Number of cases prosecuted without a warrant.

In Minnesota, for example, regular management reports can be generated from the system by any system user. Reports can be run at the state level, or broken down by law enforcement agency or court. The primary metrics reported are number of warrants submitted, approved, or rejected, as well as how many warrants were processed outside of normal court hours.

Other metrics that can be helpful are those that document the user's experience. Although these metrics typically are not built into the system itself, a short annual questionnaire or roundtable at the state law enforcement/judicial conference can be used to collect information on the following questions:

- How often did you use eWarrants or log into the system?
- How easy was it to access the eWarrant?
- How easy was it to complete/review the affidavit?
- How easy was it to submit the affidavit?

- Did you encounter any problems when preparing or reviewing an eWarrant, and if so, what were they?
- Did you encounter any problems with electronic transmission, and if so what were they?
- What changes or modifications would make the user experience better?

Finally, eWarrants are intended to provide law enforcement, prosecutors, and judges with the tools they need to effectively respond to DUI and to hold offenders accountable. These broader outcomes can be measured by tracking the following information and analyzing change over time:

- Number of refusals to submit to chemical testing
- Number of motions made to suppress BAC tests on the basis of probable cause
- Number of motions to suppress granted
- Number of DUI pleas, as charged
- Number of DUI pleas to lesser charges
- Number of DUI convictions overall
- Average length of time to disposition
- Number, type, and length of sentences given

Agencies are encouraged to collect baseline data to be able to show how eWarrant systems improve overall system efficiency and outcomes. For example, showing the amount of time that can be saved by transitioning to an electronic warrant system or reductions in warrant rejection due to errors.

Evaluation of system efficiency and effectiveness should continue on an ongoing basis. In addition to determining where future enhancements can be made, an evaluation can justify further investment in and expansion of the eWarrant system. For jurisdictions seeking policymaker buy-in or that have a desire to take a county program statewide, being able to provide data as to how the system has saved time, money, and improved overall outcomes is powerful justification for further attention and funding.

IMPROVING DUI SYSTEM EFFICIENCY

A Guide to Implementing Electronic Warrants

SECTION 7

Case Studies

SECTION 7: Case Studies

Jurisdictions interested in developing and implementing their own eWarrant system are encouraged to first examine the systems and processes in place in other localities and learn from both the challenges and successes of agencies in other states. To obtain this type of valuable insight, JMI conducted case studies in five jurisdictions that were selected based on their diversity and the nature of their systems. Each of the systems studied by JMI have unique features and operate in a slightly different manner; they also represent locally-based to integrated statewide systems.

Detailed descriptions of the development, implementation, operation, and success of eWarrant systems in Minnesota, Utah, Arizona, Delaware, and Texas are provided in the following sections.



eSEARCH WARRANTS IN MINNESOTA

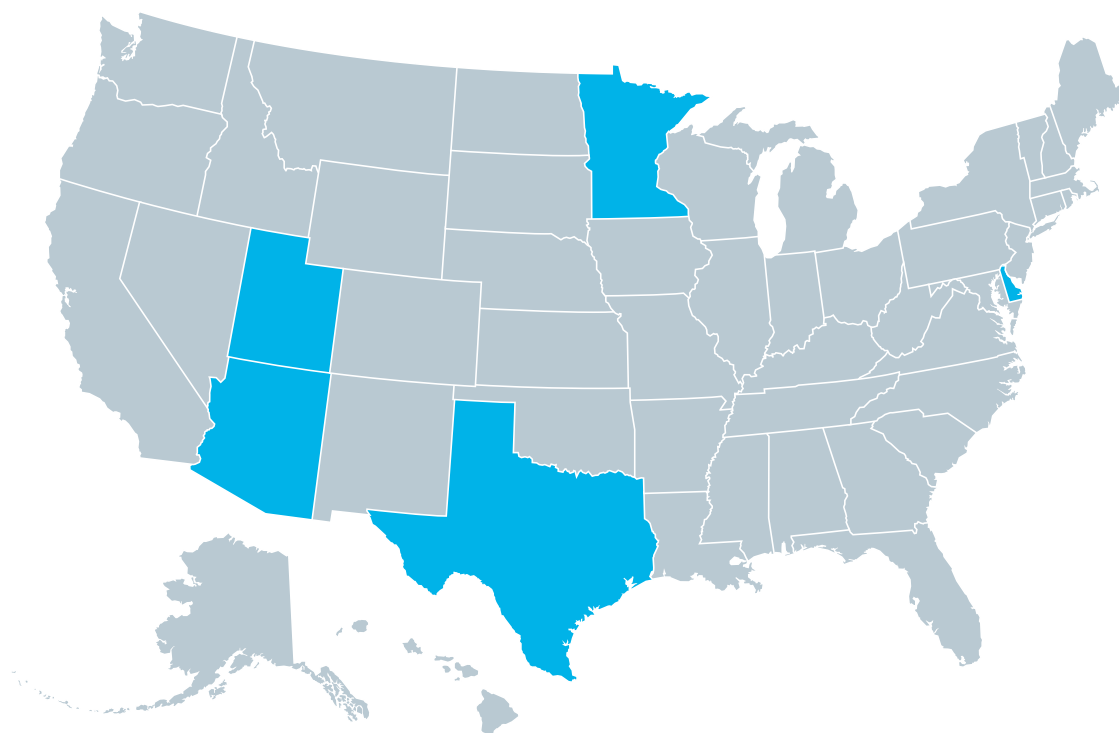
Jurisdiction profile Minnesota has a unified court system, consisting of ten judicial districts, covering the state's 86,000 square miles. The courts use a statewide electronic charging system, known as e-Charging, for criminal complaints and to move information between law enforcement, prosecution, courts, and the state driver and vehicle services department. In addition to criminal complaints and search warrants, e-Charging is used for electronic citation processing, DWI processing, and law enforcement incident report submission to prosecutors.

System development and implementation There were a number of reasons Minnesota prioritized the development of eSearch warrants for blood draws in DWI cases. In addition to court decisions requiring search warrants for blood or urine tests, the state was experiencing a growing number of legal

FIGURE 2

eWarrant Case Study Sites

 eWarrant
Implementation
Sites



challenges around blood draws and implied consent. These factors combined with a significant increase in the number of blood draw requests and the challenges to obtaining time-sensitive warrants in rural areas¹ provided the needed impetus for the creation of an electronic system. The biggest incentive, however, may have been the support and funding provided by the Department of Public Safety.

The Bureau of Criminal Apprehension (BCA) was responsible for the planning, design, and implementation of the eSearch warrant application with a \$350,000 grant from the Department of Public Safety's Office of Traffic Safety. The amount was based on a high-level estimation of development costs from concept to production and educated guesses based on previous experience with the e-Charging system.

A collaborative group of stakeholders, including law enforcement, the State Court Administrator's Office, and district court judges, worked together to draft the warrant template. Since the state had been using an e-Charging system for warrants for some time, there was not much resistance to adding blood draw warrants. However, at the outset of the e-Charging system development there was some initial resistance to new technology. To address this, a series of meetings were held with frontline staff to identify their needs and concerns in an effort to make sure these were addressed early in the process. Ultimately, by doing this, the system was designed to be highly user-friendly, which increased buy-in and acceptance. Minnesota was able to build its entire e-Charging system, including eWarrants, in-house.

TIP

Consider Local Practice

While having a statewide judicial system offers a variety of benefits, the eWarrants system must be flexible enough to accommodate local practices. What works well for urban areas may not work as well in rural parts of the state.

The roll-out of eWarrants for DWIs began in October 2016 with a 3-month pilot program, first with the Minnesota State Police in Hennepin County (the most populous county in the state), which includes Minneapolis. By mid-November 2016, eight municipal police departments had been added to the pilot, with successive roll-outs across the state by judicial district. By April 2017, the system had gone statewide.

System operation

Similar to other jurisdictions, officers seeking a warrant for a blood test² log onto a secure portal³ to complete and submit an electronic search warrant application to a judge. Officers were provided with a mobile data computer to use in their car to allow access to the system while at the arrest scene so they could request warrants at any time, day or night. Screen shots of the log-in screen, along with a screen shot of the officer's work station he/she sees upon login, are provided below and on the following pages.

FIGURE 3

Minnesota eCharging Login

FIGURE 4

Minnesota eCharging Work Summary

© 2013 BCA [Privacy Statement](#) [Help](#) Version 3.0

The officer then selects the type of document he/she wants to create and is brought to a DWI wizard for DWI arrests. The wizard then prompts the officer to enter the peace officer certificate (a hero statement), incident details, additional forms, and signatures as shown on the left side of the screen shot on the next page.

TIP

Consider Boilerplate Language

eWarrants in Minnesota contain boilerplate language on dissipation rates for alcohol and controlled substances so that the officer does not need to enter this information each time. The ability to access and insert this type of language increases efficiency and can save officers valuable time.



FIGURE 5

Minnesota eCharging DWI Wizard

The screenshot displays the eCharging application interface for the 'DWI Wizard - Breath Test Advisory' step. The interface includes a navigation menu on the left, a main content area with a form, and a top navigation bar.

Top Navigation Bar:

- Current Agency/District: Cook County Sheriff
- Search: First/Last name or Case/Citation #
- Welcome Kent Coptest
- Logout

Navigation Menu (Left):

- My Work
- Manage Forms
- Notifications
- Preferences
- Reports
- Help
- DWI Wizard - Breath Test Advisory (2 of 11)
- Subject Lookup
- Subject Details
- Breath Test Advisory
- Peace Officer's Certificate
- Vehicle Details
- Incident Details
- Forms Summary
- Form Details
- Sign Forms
- Finish Decision
- Assignment
- Attachments
- Publish / Archive
- DWI Summary
- Advanced Search

Main Content Area:

Assigned to Law Enforcement (click for history)

Responsible Agency: **Cook County Sheriff**

Document Type: DWI Form	Case Numbers:
Defendant: AL EDWARD TWO	Law Enforcement:
eCharging Id: 63570	Prosecution:
Document Id: 14362	Court:

Buttons: Back, Next, Save, Assign, Help

Type of Incident

Was the offender operating a commercial vehicle? No Yes

If the offender was operating a snowmobile, ATV, or watercraft, do not process this incident through eCharging.
For Off-Road Recreational DWIs, you must use the paper forms provided by the Department of Natural Resources (DNR). These are available for download from the **Available Documents** list on the eCharging login page.

Opt Out of Breath Test Advisory

If the Breath Test Advisory was not read, check this box. **Previously entered Breath Test Advisory data will be lost if this option is selected.**

FIGURE 6

Minnesota Draft DWI Search Warrant

Draft (click for history)

Document Type: DWI Search Warrant
Defendant:
eCharging Id: 28811
Document Id: 1780

Case Numbers:
Law Enforcement: 20161223
Prosecution:
Court:

Print Preview Help

Incident

Subject Details

First Name: *
 Middle Name:
 Last Name: *
 Suffix:
 Date of Birth: *

Date and Time of Incident

Date of Incident: *
 Time of Incident (Military time): *

Location of Incident

Describe the location of the incident*

East Bound I-194 between Normandale Blvd and France Ave South

Enter up to 500 characters. 434 remaining.

City or Township of*
 County of*
 State of Minnesota

Reason for Initial Contact

Check at least one of the following.*

Vehicle stopped by officer, because:

Accident

Vehicle already stopped, because:

Other:

The system is designed to interface with the state department of motor vehicles (which in Minnesota is called Driver and Vehicle Services) so that the officer can conduct a search based on name and date of birth to confirm the identity of the suspect and auto-populate the demographic fields (address and driver's license information) as well as the vehicle information. The officer then indicates the offense level (felony/misdemeanor) and a case number is added for later use in the e-Charging system. Screen shots of the system are provided on the following pages; additional screen shots can be found in [Appendix F](#). Similar to Utah's system, the county entered into the system by the officer provides a drop-down list of available judges who can receive the warrant for review. In rural areas, there is typically one judge who receives warrants from all counties within the district.

“

“Minnesota has rolled out eWarrants over the past few years and it has dramatically improved our responses. Our judicial district stretches over the entire arrowhead region of Minnesota, with one-way drive times sometimes measured in hours. The ability for law enforcement to connect with a judge to review warrants electronically rather than for in-person review has been a tremendous time saver. Officers are spending their valuable time in the field, not driving to meet the judge.”

—Judge Shaun Floerke, Sixth Judicial District Court, Duluth, Minnesota

FIGURE 7

Minnesota DWI Warrant Application

My Work Manage Forms Notifications Preferences Reports Help

Search Warrant - Application Search Warrant Details Save successful

Search Warrant Type
Search Warrant Application
Advanced Search

Draft (click to history)

Document Type: DWI Search Warrant Case Numbers: Law Enforcement: 20181018
 Defendant: AL EDWARD TWO Prosecution: Court:
 eCharging Id: 01399
 Document Id: 229

[Print Preview](#) [Help](#)

Description Grounds Facts Additional Requests

Warrant to Search:

Select all applicable

Premises
 Motor Vehicle
 Person

First Name: Middle Name: Last Name: Suffix: Date of Birth:

AL EDWARD TWO [v] 01/01/1974

Property and Things to be searched and seized:

List all the evidence that needs to be searched and seized

Formats: [v] [v] [v] [v]

Blood sample from AL EDWARD TWO, Date of Birth 01/01/1974

Description of premises, motor vehicle or person to be searched, where the above evidence will be found:

List and describe in detail the premises, motor vehicle or person - where the above evidence will be found.

AL EDWARD TWO, Date of Birth 01/01/1974

Location of Search

City or Township of: County of: Hennepin State of Minnesota

[Save and Continue](#) [Save](#)

FIGURE 8

Minnesota eWarrant Signature

Currently Assigned to: Dev Officer, at the Carver County Sheriff

Sign and Submit to Judge

I declare under penalty of perjury that everything stated in this document is true and correct.

Place of Signature
 County: State:

Officer's Call back phone# (This phone number will only be visible to the assigned Judge.)

Select Judge
 Courthouse: Judge:

2, Judge
 3, Judge
 Carverjudge, Karen
 Dredd, Judge
 Jones, Judy
 Judge, Biometric
 Judge, DA
 judge, djc
 Judge, GT
 Judge, KR
 Judge, KS
 Judge, TM
 Judge, Tom
 judge, winona
 judge1, carver
 judge2, carver
 Schoen, Paul
 Vel1, JRams
 Vel2, JRams
 Vel3, JRams

Application Page 1 - 2

STATE OF MINNESOTA, COUNTY OF CARVER

DISTRICT COURT

APPLICATION FOR SEARCH WARRANT

The on-call judge receives an email with a hyperlink directly to the warrant in the system, or if after normal business hours, an email notification about a pending application. However, judges can only access the system if they are on a court device, using a secure network. During the initial roll-out of the process, upon receipt of the request, the judge called the officer by phone to swear them in. That requirement was eliminated in 2017 when the Minnesota Legislature recognized penalty-of-perjury law enforcement signatures for search warrant applications.

After reviewing the warrant, the judge may either issue it by applying an electronic signature or reject the application. If the warrant is denied, the judge must include the reason(s) for denial. The officer receives a notification that the warrant has been returned and if it was rejected, he/she may either correct the warrant and resubmit, or in some cases determine that the warrant will not be resubmitted.

The system also includes document history so officers can view the status of the warrant. If a judge has not taken possession of the warrant, there is an option to recall it to correct any errors. Doing so, however, requires the officer to re-sign and resubmit the request to assure that the latest document version is always processed. Once approved, the officer can print the warrant in his/her vehicle and take it to a medical facility for the blood draw.

System success The use of electronic warrants has significantly streamlined the process and staffing required to obtain a blood draw or urine warrant. Experienced officers typically can prepare warrants in 10 minutes or less, and officers report the average processing time, from submission to judicial approval, is between 15-20 minutes for warrants that do not have any issues or problems.

Since the eSearch warrant became available, Minnesota law enforcement officers have submitted over 2,500 applications for DWI-related search warrants. Ninety-eight percent of those applications are approved and result in the judge issuing a search warrant. In addition, the error rate on DWI forms has been reduced from 30% to nearly 0%. Users of the system report the electronic system has made the process of reviewing search warrant applications faster, more efficient, and more secure. Approximately 55 to 60 eWarrants are issued statewide each day, up from 20 when the process was done manually using paper.

The BCA's eSearch warrant application recently received the 2017 State Government Innovation Award as one of the top innovation projects in state government. The eSearch warrants allow the entire search warrant application and approval process to be completed electronically, resulting in improved efficiencies, greater security, and measurable savings in time and money.⁴

Results of eSearch in Minnesota

- 2,500 eSearch warrants submitted in one year
- 98% of requested warrants were issued
- 11,200 office hours saved
- 30-minute reduction, on average, in DWI arrest processing time
- Decrease in percentage of DWI forms with errors from 30 to nearly 0%

UTAH CRIMINAL JUSTICE INFORMATION SYSTEM (UCJIS)

Jurisdiction profile Utah is geographically a large state with 29 counties and 8 judicial districts. The entire population of the state is just over 3 million people. The state court system introduced an electronic warrant pilot program in the spring of 2008, in response to *State v. Rodriguez*, 156 P.3d 771 (2007), a case in which the defendant turned into the path of a school bus killing her passenger. The driver, smelling of alcohol and acting belligerent, was taken to the hospital where her blood was drawn without her permission. She was revealed to have a BAC level of .39 – nearly five times the legal limit. The driver was convicted of a 2nd degree felony. Although her conviction was overturned on appeal, it was subsequently reversed affirming the conviction. In issuing its opinion, the Utah Supreme Court issued a strongly worded statement, “We are confident that, were law enforcement officials to take advantage of available technology to apply for warrants, the significance of delay in the exigency analysis would markedly diminish.”

System development and implementation In response to the *Rodriguez* decision, the Utah Department of Public Safety (DPS), the Salt Lake City District Attorney's Office, and the Administrative Office of the Courts (AOC), with collaboration from judges, came together to build an eWarrants system to speed up access to warrants in DUI cases. Since more than 90% of state law enforcement is connected to the Utah Criminal Justice Information System (UCJIS), which unifies data from dozens of separate data sources and agencies, the decision was made to incorporate the eWarrants system into the UCJIS platform using open source code (meaning there was no copyright or license),⁵ integrating it with other relevant services.

A Justice Assistance Grant (JAG) of \$30,000 was provided to DPS to hire a contractor for the additional programming, which was supplemented with additional JAG funds increasing the total grant to \$34,693. Another JAG grant of \$49,511 was awarded to the AOC, although they ultimately only used \$25,250 of the award, to develop the system. Additional and ongoing funding comes from impound fees, mandated by state legislation.

“

“The eWarrant system has resulted in officers’ willingness to get a warrant because the system is very simple and efficient. Getting a warrant does not interfere with the DUI process like it did in the past. Before the eWarrant system was implemented most officers would not go through the hassle and effort to get a warrant unless it was a very serious case involving injury or death, and now we attempt to get a warrant on every refusal.”

—Trooper Jason Marshall, Utah State Drug Recognition Expert
Coordinator

System operation

Patrol cars in Utah are equipped with computer terminals with Internet capabilities that officers use to log into UCJIS to initiate the warrant request. Each officer has an assigned username and security token that is tied to his/her qualifications and training, allowing the hero statement of the officer’s training and qualifications in the warrant, to be auto-populated. The remainder of the warrant includes both drop-down menus and text fields to streamline the process, save time, and reduce errors (a series of screen shots showing the Utah eWarrant system is included in [Appendix A](#)). Officers have the option to send the warrant to a prosecutor for review prior to submission or they can check a box to skip this step and transmit directly to a judge.

The state uses a rotation system for assigning judges to review warrants. Typically, judges are assigned 1-2 weeks per year, and there are 7-8 judges on-call 24 hours a day, 7 days a week. When the officer chooses the jurisdiction and county in which the warrant is being issued, the UCJIS system automatically selects one of the on-call judges and adds the judge’s contact information in the event the officer does not receive a return response in a short period of time. The system then generates a text and email message that is sent to the assigned judge to notify him/her there is a warrant pending review.

Because Utah changed its administrative rules of criminal procedure⁶ to allow officers to be sworn in digitally, the officer’s electronic signature line added to the penalty of perjury statement eliminates the need for administering the oath in-person or via video call. Thus, upon receipt of the warrant, the judge can promptly review and affix his/her electronic signature if the warrant is approved and return it electronically to the requesting officer. If the warrant is rejected, the judge notes the reason for rejection. One of the many useful features of the UCJIS system is that the officer has the ability to initiate queries to see the status of warrants including dates and times of submission, review, approvals, and rejections. Figure 9 illustrates this process from start to finish.

TIP

Reduce Common Errors

UCJIS requires that drivers’ license numbers be entered twice to reduce typographical errors.



FIGURE 9

Utah eWarrant Workflow

- 

1 Officer logs on to UCJIS, enters information. Includes District on-call judge to be notified, return contact info (email, pager, text msg to phone).
- 

2 Prosecutor (notified via email, pager) reviews information, works with officer to make any adjustments required.
- 

3 After review with prosecutor, notification is sent to on-call judge via email/text msg to pager/cell phone. Msg contains ID number eWarrant.
- 

4 On-call judge logs on to UCJIS, accesses eWarrant by ID number (or can select from list).
- 

5 Judge approves eWarrant, updates document to indicate approval. Stored on UCJIS server as non-modifiable PDF. The warrant is also sent immediately to the Courts.
- 

6 Notification is sent to initiator via email/text msg to pager/cell phone that eWarrant is approved/issued. Notification contains ID of eWarrant.
- 

7 Officer logs on to UCJIS, retrieves eWarrant, prints out to serve it.
- 

8 After serving warrant, officer enters "return of service" information which is forwarded to the Courts. If no return of service info entered within a determined amount of time, notification to do so will be sent (via email, pager, text msg to phone).

System success The entire process averages 20 minutes from request to judicial approval, although it can take up to an hour. With the implementation of eWarrants, Utah has improved its test submission rate from 77% to 96% (Berkovich, 2015). There has also been tremendous buy-in from stakeholders on the use of the electronic warrant system in Utah, especially in rural areas where there is limited access to judges. Notably, having electronic warrants has eliminated the need to have affidavits read over the phone to judges and because everything is now logged in electronically, including the return of service, the process is more secure. Law enforcement in rural areas, with limited internet access, have been provided with SIM cards to improve their communication abilities and report no hardships associated with eWarrants.

The state has convened an eWarrants committee, consisting of IT, law enforcement, prosecutors, and court personnel, to keep abreast of legislation and identify ways to continue to improve upon the process. The Bureau of Criminal Identification (BCI), the steward of UCJIS, pays the costs of enhancements.

TIP

Anticipate Rural Challenges

Rural counties may face unique challenges on account of limited resources, fewer staff, and less cell/internet coverage. Identifying these limitations and planning/budgeting accordingly is encouraged.

eSEARCH WARRANT AND eRETURN APPLICATIONS IN MARICOPA COUNTY, ARIZONA

Jurisdiction profile Maricopa County (Phoenix), Arizona has an estimated population of 4.186 million residents. The Phoenix Police Department alone handles around 6,100 DUI cases per year. The development of the eSearch warrant and eReturn Applications for blood draws in DUI cases began in the summer of 2011. The Maricopa County Superior Court and Phoenix Police Department held three informational sessions with law enforcement to collaborate on the design, development of policies, and implementation of the system.

System development and implementation In 2012, the Presiding Judge of the Superior Court in Maricopa County issued an administrative order authorizing a two-year electronic search warrant pilot for the “exchange of search warrants, affidavits, and returns by law enforcement officers and the court by means of a secured internet connection”⁷ (a copy of the administrative order is included in [Appendix F](#)). In August of 2012, local law enforcement agencies were invited to participate in a pilot program to test the eWarrant process and the application. The initial pilot test was conducted with one Phoenix police DUI officer. By September, all Phoenix Police Department DUI Squads were using the application.

Working with the courts, the Phoenix Police Department prepared a training video for law enforcement officers on the eSearch warrant and eReturn process. By December of 2012, the entire Phoenix Police Department had been trained on how to use the applications and was using both. One year later, there was gradual deployment to additional law enforcement agencies within Maricopa County. The pilot project became permanent by Local Rule 4.10, effective May 28, 2014. Once the eSearch warrant and eReturn applications were made permanent, it was expanded to include all Department of Public Safety (DPS) law enforcement officers across the entire state to allow them access to the system.

The Superior Court received two grants from the Governor’s Office of Highway Safety to develop the software and enhance the law enforcement officer website to include the return of service. The first grant was provided in the amount of \$30,576 to build the software for Maricopa County Law Enforcement Agencies. This also covered training costs and materials. The second grant was provided by the State Administrative Office of the Courts in the amount of \$87,838 to modify the software to enhance the application for use by DPS statewide and to fund the Judicial Officer and Judicial Assistant salaries/benefits for 15 hours per week to cover the increase in workload for services delivered outside of Maricopa County.

System operation The eSearch warrant application was designed and programmed in-house by the court information technology department as part of the court’s information system. Officers are assigned a serial number to access the application via the Internet. The application includes a series of checkboxes and pull-down menus that allow the officer to indicate the type of offense, qualifications and training, probable cause for the stop, roadside tests administered, suspect behavior, and refusals. Figure 10 provides a screen shot of the initial data entry screen. Officers also have the ability to view the status of their warrant requests online.

The Phoenix Police Department alone handles around 6,100 DUI cases per year.

FIGURE 10

Arizona Affidavit for Search Warrant Status

2/5SW User: [redacted] Group: IA Judicial Officer

Mark work queue item status to complete? [Back to Queue](#) Status: In Progress

Affidavit For Search Warrant - Status: Warrant Granted

Do Not Seal

Phone # (602)320-XXXX Search Warrant # SW2013-XXXX
Report # 2013 01-XXXX

YOUR AFFIANT, [redacted] - #XXXX deposes and says: I am investigating the crime of:
 DUI/APC Aggravated DUI Aggravated assault Manslaughter Homicide Endangerment
 which occurred on or about 8/12/2013 1:04:00 AM, at [redacted] W. CAMPBELL in the City of Phoenix, County of Maricopa, State of Arizona

THAT THE AFFIANT has probable cause to believe that there is now in the blood or bodily fluids of:

Name	Race	Gender	DOB
[redacted]		Male	10/7/1979

located at: [redacted] E. HIGHLAND or at any other location while in police custody, in the City of Phoenix, County of Maricopa, State of Arizona

The following substances of wit, intoxication liquor, drugs, vapor releasing substance or any combination. Together with other evidence of the crime of:
 DUI/APC Aggravated DUI Aggravated assault Manslaughter Homicide Endangerment

As set forth in the affidavit, I [redacted] - #XXXX, your Affiant, am a Peace Officer in the State of Arizona, employed by the Phoenix Police Department. I have been a sworn officer for 20 years and have the following training and experience:

I graduated from: **The Phoenix Police Academy**

My training included identifying driver impairment due to alcohol or drugs. My duty assignments have included traffic, criminal and DUI investigations. I have specialized training in:

H.G.N. (Horizontal Gaze Nystagmus) D.R.E. (Drug Recognition Expert)
 [redacted] [redacted]

Once completed, the affidavit is sent electronically to a judicial officer for review, and approval or rejection. Judges receive notice of a pending request and can log onto the system into their “work queue,” which shows affidavits they have received and their status (i.e., new, in progress, completed). Judges also have the option to filter the view in their workstation to show only new affidavits as well.

FIGURE 11

Arizona eSearch Work Queue

The screenshot shows the Arizona eSearch Work Queue interface. The top navigation bar includes a menu icon, the iCIS logo, and a 'Work Queue' title. A red arrow points to a '1/3SW/1' indicator in the top right corner. The main content area features a sidebar on the left with navigation options: IA PSA (3002), Search Warrant (31), Petition to Revoke (7), Jail Fingerprint (6), and PSI Report (4). The main area displays a table of search warrants with the following columns: Record Info, Type, Status, and actions. The table contains three rows of data:

Record Info	Type	Status	As	St	Er	Actions
(480) 912-0000 SW2013-00000 Return Verified (10/28/2013 04:32 PM)	Search Warrant	New				Work On Claim Cancel
480-0000000 - 21236 SW2013-000000 Warrant Granted (10/29/2013 08:55 AM)	Search Warrant	New				Work On Claim Cancel
(602) 912-0000 SW2013-00000 Return Verified (10/29/2013 09:18 AM)	Search Warrant	In Progress				Work On Unclaim

The bottom right corner of the interface shows 'Displaying items 1 - 3 of 3'.

Using the same system, officers are also able to submit a return of service to the judicial officer to verify. The system allows the return to be sealed electronically and includes checkboxes for the property that was seized (i.e., blood, urine, other items); a checkbox indicating the warrant was not served; and electronic certification of the search warrant execution. (See next page for a screenshot of the eReturn application).

FIGURE 12

Arizona eSearch Return Verified

Once a warrant is granted, the driver's blood is taken by an officer trained in phlebotomy to do the procedure. If the officer has not been trained⁸, there is either a phlebotomist with him/her, or they will transport the suspect to a medical facility.

Mark work queue item status to complete? [Back to Queue](#) Status: In Progress

Return Of Search Warrant - Status: Return Verified

[Search Warrant.pdf](#) [Search Warrant Issuance.pdf](#) [Search Warrant Affidavit.pdf](#) [Search Warrant Return.pdf](#)

Seal

Search Warrant # SW2013-
Report # PPD-2013-0000000000

I certify that on 10/29/2013 this warrant was executed and the following described Property was seized:

3 tube(s) of blood
 urine sample
 other item(s) as described below
 Warrant was not served

I further certify that the foregoing inventory is a true and detailed account of all property taken by me, pursuant to ARS § 13-3921, and that a detailed receipt for the property taken was:

given to: left at: [Name], [Address], Caucasian, Male, 11/11/1970.

Rule 2.13 of the Local Rules for the Superior Court in Maricopa County authorizes the court to use electronic oaths and such oaths have the same legal effect as a signed oath or an oath taken in the presence of a judicial officer.

I, [Name], do solemnly swear or affirm that the information located on this return is correct and complete, and that I have personal knowledge of the information on this return.

Dated 10/29/2013

System success The average time to secure an electronic warrant using the Maricopa County system is between 15-20 minutes. Since implementation, there has been a 13% increase in DUI search warrants.

The court's Search Warrant Center (initial appearance court) is staffed 24 hours a day, 7 days a week. By June 2018, the software will be modified to allow all 14 counties and all cities in Arizona access to use the DUI eSearch warrant and eReturn applications. This will increase the volume of requests for DUI search warrants, and it is anticipated that additional funding will be provided to fund the increased workload for the Judicial Officer and Judicial Assistant.

Since implementation, there has been a 13% increase in DUI search warrants.

DELAWARE JUSTICE INFORMATION SYSTEM (DELJIS)

Jurisdiction profile

The state of Delaware is unique on account of its size, structure, and population density. It is the second smallest state and is comprised of only three counties. While it is the sixth least populous state, it is also the sixth most densely populated. Given these characteristics, Delaware was well-positioned to create a statewide information-sharing system. In fact, according to a report of the National Task Force on Court Automation and Integration, Delaware was the first state to implement an integrated criminal justice information system that supported electronic sharing of criminal justice information among the criminal justice community. The Delaware Justice Information System (DELJIS) has been in existence since 1983, and it is constantly changing to meet the needs of system participants, including law enforcement. It is therefore not surprising that the implementation of eWarrants was built into the DELJIS platform, making Delaware one of the first states to use automated warrants.

System development and implementation

Delaware implemented an automated warrant system in 1991, allowing law enforcement officers to enter complaint data through a mainframe system using Microsoft Word fillable forms to create warrants on-line. In 2013, shortly after the *McNeely* ruling, the state began to implement processes to use electronic warrants for blood draws in DUI cases. DELJIS converted the Microsoft Word form into a PDF and housed it on its system. The request for adding blood draw eWarrants to DELJIS was accelerated through the issuance of a policy memo by the Chief Magistrate. The design and implementation was truly a collaboration of the courts, DELJIS, the state prosecutor, and state and local law enforcement.

The costs for automating and incorporating warrants into the DELJIS platform were absorbed into the DELJIS budget as a part of routine system improvements. Thus, the primary cost to the state was for equipment to allow law enforcement to access the system remotely. In 2011, the Delaware Police Chiefs Council (the Council) first requested funding for the lease of laptop computers for all Delaware police departments, excluding the Delaware State Police. In subsequent years, requests have been made for other equipment in addition to the funding for the lease of the computers. The Council is currently in the fourth and final year of the current lease. The amount

requested each year under the current lease is \$340,220, which provides for 970 computers and includes a buyout at the end of the lease of \$1. Including the buyout allows departments to keep the old laptops, which saves a significant amount of work collecting the old units, also saving on return shipping costs. In addition, DELJIS receives \$250,000 a year for maintenance on the systems from court assessed fees. These costs are recovered by assessing a \$1.00 fee on each adjudication of guilty, delinquency, or responsible action for all crimes.

System operation

Law enforcement officers access DELJIS and the eWarrant form with a secure sockets layer (SSL) account through the Internet using laptops, tablets, and desktops. Upon logging into the system, officers enter the suspect's name and date of birth. The DELJIS system automatically searches for the individual to find additional information including criminal history and can access the state's department of motor vehicles records as well. Officers then complete the remainder of the request using fillable fields on location of incident, actions of the defendant, statements made, and other facts supporting probable cause. A PDF document is produced, which is then faxed to the on-call judge. The on-call judge swears the officer in via video conference. After review and approval, officers receive the signed PDF via fax. Judges use their bar code as an electronic signature.

Each county has a contract with a phlebotomist who will come directly to the station or the hospital to draw the blood. It generally takes the phlebotomist between 20 minutes to 2 hours to arrive, with the average time being 30-45 minutes. If the suspect has been transported to a hospital, hospital policy will not allow for a forcible blood draw if there is no consent, even if there is a warrant. The use of eWarrants in Delaware requires a law enforcement officer, court staff, an on-call magistrate, and a phlebotomist.

System success. The incorporation of eWarrants into the DELJIS platform has made the process of obtaining a warrant in DUI cases extremely efficient. DUI blood draw warrants receive priority within the system, and the average turnaround time is approximately 8 to 10 minutes. The longest time recorded for the issuance of a warrant since the implementation of eWarrants was 34 minutes.

DELJIS staff is responsible for maintaining the system and making updates to it. One of the updates planned for late 2017-early 2018 is a change to login authentication. Delaware is moving from one-factor identification, which is just a user id and password with an SSL account, to a two-factor system, which generates a number that changes every minute, in conjunction with the user id, and password. Preliminary testing indicates increased security with the two-factor identification and enthusiasm among law enforcement. This process will require officers to download an application to their phones or a “token” to generate the number and will increase security.

TIP

Identify ways to enhance the existing system

As policies, protocols, and technology evolves, it is important to determine whether changes should be made to ensure the system continues to meet practitioner needs. Stakeholders are encouraged to convene to proactively identify limitations and potential system enhancements.

ELECTRONIC WARRANTS IN TEXAS

Jurisdiction profile Texas is the second largest state in the United States. There are 266,597 square miles in Texas, and it has a population of 27,862,596. Texas does not have a unified court system; each of the 254 counties is responsible for their own criminal justice and court systems, resulting in a patchwork of practices, policies, and results. Several jurisdictions in the state have worked to implement eWarrants. Two counties in Texas – Montgomery County and Lubbock County – have implemented eWarrants as a tool to enable the state’s No Refusal program,⁹ after the practice was ruled unconstitutional by the Texas Criminal Court of Appeals in 2014, because blood was being drawn without a warrant. Both of these systems are highlighted.

System development and implementation Montgomery County, Texas, a growing county in the Houston metropolitan area, responded to the Court’s ruling by developing an automated system to request warrants electronically via the Internet. The Montgomery County District Attorney worked with Document Logistix, a document management company, to create the application called Mynorefusal.com. The District Attorney contacted Document Logistix with the idea of creating a low-cost eWarrant and consulted with them to create mynorefusal.com, which is now available at no charge to those wishing to use it.

System operation Officers log into mynorefusal.com, either by phone or laptop, and using a series of drop-down menus and open text fields provide details about the alleged offense, evidence, results of SFSTs, and other factors relevant to establishing probable cause. The drop-down menus include facts supporting probable cause (such as odor, facial appearance, speech, attitude, balance, open container, etc.) and checkboxes for the standardized field sobriety and horizontal gaze nystagmus tests and results. The warrant is then signed electronically (typed name followed by “/s”) or written by hand on the computer screen if touch screen capability exists. [Appendix F](#) contains two additional screen shots showing the SFSTs entry, other factors, and the affiant screens.

NOT JUST FOR WARRANTS

An additional feature of the Mynorefusal application, once the warrant is issued, includes system generation of booking documents for the jail and for license revocations.



FIGURE 13

Texas No Refusal Search Warrant Affidavit

The screenshot shows a web browser window with the URL mynorefusal.com/home?NSAIDivAffidavit. The page title is "New Search Warrant Affidavit". The form is divided into several sections: "Offense", "Evidence", "SPSTs", "Other Factors", and "Affiant". The "Evidence" section is active and contains the following fields:

- Odor: * (Dropdown menu: Mild/None)
- Face Appearance: * (Dropdown menu: Flushed/Normal)
- Speech: * (Dropdown menu: Slurred)
- Attitude: * (Dropdown menu: Calm/Agitated)
- Balance/Walking: * (Dropdown menu: Normal/Off)
- Drinking period (time): (Time range: 12:00 PM to 2:00 PM)
- Drinking Location: (Text field: Office Party)
- Types of Alcoholic Beverages: (Text field: Bourbon)
- Open Containers (inside vehicle): (Text field: No)
- Other Indications of Mental Impairment: (Text field)
- Suspect Statement: (Text field)
- Other Evidence of Drug Use: (Text field)

At the bottom right of the form, there are "Next" and "Prev" buttons. The footer of the page reads "© 2017 - No Refusal".

Once signed, the system generates a PDF document which is transmitted to a judge by email or fax. The judge receives an email and a phone notification of the pending warrant for review. The appellate court recently approved language on warrant rejection which will be added into the system to allow the judge to provide the reasons for rejection back to the officer electronically.

System success With the implementation of mynorefusal.com, law enforcement officers are now able to publicize and operate the No Refusal Program. Since the eWarrant capability has been developed, there has been a significant decrease in the number of individuals who refuse breath or blood tests. In addition, the District Attorney (DA) who developed mynorefusal.com notes that defense attorneys now inform potential clients about the ability of law enforcement to quickly obtain warrants for blood draws and advise them to submit to breath testing rather than face the warrant.

Implementation of mynorefusal.com has reduced refusals, which in Montgomery County alone were estimated to be about 59% during periods in which the No Refusal Program was not operating. In 2015, of the 25 DWI cases that went to trial, 20% had BAC warrants, 40% voluntarily submitted to BAC tests,

and the remainder involved refusals in which no sample was obtained. In that year, the District Attorney's Office had an 80% conviction rate in DWI cases. During 2016, 42% of DWI cases that went to trial had BAC warrants and 28% voluntarily submitted to BAC tests. The 2016 conviction rate increased to 89%.

System development and implementation Lubbock, a city of about 242,000 in the northwestern part of the state, has also developed a system to expedite warrants electronically. The Lubbock electronic warrant system began in 2012 with a trial period which lasted about 6 months. The Lubbock DA developed a form law enforcement could access on their laptops to generate a warrant. Initially, the officer visited the judge to get the warrant signed, but as stakeholders became more comfortable they began to introduce emailing the warrant to judges. The Lubbock police department trained both officers new to the procedure and judges on the electronic warrant system. During the trial period, modifications, such as adding the suspect's name in addition to the file number, were made. Lubbock encountered no significant costs associated with implementing electronic warrants other than the time the officer spent learning the system.

Mynorefusal.com Outcomes (2015-2016)

- 11% increase in DWI conviction rates between 2015 and 2016
- 52% increase in DWI cases with BAC tests results obtained with a search warrant
- 30% decrease in the number of DWI cases that went to trial in which defendants refused to submit to blood tests and no sample was obtained

System operation

Once an officer has made a stop and determines probable cause exists to request a blood draw warrant, the officer will write an affidavit on a department issued tablet. Initially, touch-screen laptops were used, now most officers have tablets. The affidavits are standard forms with drop-down menus, as well as text fields. The law enforcement officer must be sworn in by another officer, or by a notary.

Some judges will swear the officer in over the phone if they are confident they recognize the voice of the officer. Once the judge receives a call, or email alert, that there is an affidavit for review, the judge retrieves it in a PDF document. After it is approved, the judge affixes his/her signature and includes a printed name, date, and time. The approved warrant is then faxed or emailed back to the officer. In addition, the warrant may also be returned with an order for assistance for medical personnel to conduct the blood draw, with or without consent.

System success

On average, warrants in Lubbock County are being processed within 5 to 10 minutes saving officers valuable time. Following the successful implementation of the Lubbock Police Department electronic system, other law enforcement agencies, including the Texas Department of Public Safety, Texas State University, and the Texas Department of Wildlife, expressed an interest in using the warrant process created by the Lubbock District Attorney.

Each of the preceding are examples of eWarrant systems that have improved the efficiency of the DUI arrest process and produced promising outcomes in their respective jurisdictions. These models range from comprehensive statewide integrated systems to simple processes at the county level. Agencies that are interested in establishing their own system can adapt these models to fit their own individual needs and are encouraged to select the approach is most feasible based on existing infrastructure and resources. Expansion of these systems to incorporate additional agencies or jurisdictions is a goal to work towards.

¹ In Minnesota, an .08 alcohol reading within two hours of driving ensures arrest and revocation of privileges.

² Minnesota statute allows for the officer to choose either blood or urine to test.

³ When the system was originally implemented the log-in process was biometric, which has since been augmented with the assignment of user name and passwords. Officers and judges still have the option of a fingerprint login, which many still use.

⁴ <https://dps.mn.gov/divisions/bca/Pages/default.aspx>

⁵ The use of open source code creates the opportunity for other jurisdictions to use the program and tailor it to their needs.

⁶ Utah R. Crim. P. Rule 40: "remotely communicated warrants" may be issued "when reasonable under the circumstances"; a request to the magistrate may be made by "voice, image, text, or any combination of those, or by other means"; testimony is to be under oath and recorded, which may be "by writing or by mechanical, magnetic, electronic, photographic storage, or by other means"; the magistrate may direct the applicant to sign the magistrate's name, and the warrant and recorded testimony shall be retained and filed with the court.

⁷ <https://www.azcourts.gov/Portals/22/admorder/orders12/2012-15.pdf>

⁸ Most Maricopa officers have been trained as phlebotomists and are able to conduct blood draws.

⁹ The No Refusal program was initiated in Harris County, Texas (which includes the city of Houston) by law enforcement and the District Attorney's Office in response to the high rate of BAC test refusals. At the time the program started, refusals were estimated to occur in 35 to 55% of DUI stops.



SECTION 8

Troubleshooting and Mitigating Unintended Consequences

SECTION 8:

Troubleshooting and Mitigating Unintended Consequences

The implementation of new processes and systems inevitably produces some challenges as well as unintended consequences. Knowing what challenges may arise early in the design and implementation stages can help offset long-term impact as well as mitigate any unintended consequences.

TROUBLESHOOTING

Although it is impossible to predict every conceivable challenge a jurisdiction may face when implementing an eWarrant system, there are a number of common issues that jurisdictions studied by JMI experienced. These include:

- Outdated computer systems
- Resistance to new technologies
- Lack of consensus about the format of the eWarrant form

Outdated computer systems are perhaps the biggest obstacle in creating eWarrant systems, either in terms of building onto an existing platform or linking with other information systems operated by allied stakeholders such as the courts, criminal history repositories, or state driver licensing authorities. Many criminal justice agencies, and courts in particular, operate on legacy systems. These antiquated systems rely on old technology, old programming and methods, and adding new features or creating bridges to access data is almost impossible. This was the situation Washington State faced as it was designing and implementing its DUI packet – the court’s information system was outdated and could not support additional forms, reporting, or data exports to outside systems. Luckily, a collaborative approach was used in the planning and design, and, as a result, the issue was identified early in the process and plans were put into place to request funding for a new information system for the court. Although there will be delays in making the connection, it will not slow the implementation of eWarrants overall.

Another common challenge is overcoming resistance to new technologies. Frontline staff as well as supervisors in law enforcement, prosecutors, and judges may be reluctant to try new systems and technologies. Reasons for their reluctance can vary from simple discomfort or unfamiliarity with new hardware to poor experiences with new technologies that historically have negatively impacted workload. Early engagement of individuals who will use the system is imperative to identify their expectations, needs, and concerns. This is the first step in preparing for resistance and devising a strategy to manage and/or overcome stakeholder apprehensions. Ongoing engagement in pilot testing and evaluation as well as targeted training is important. Minnesota, for example, spent a significant amount of time upfront conducting one-on-one meetings with frontline users to assess concerns prior to implementation.

The final challenge jurisdictions commonly face arises over disagreements about format. The eWarrant itself is often the focus of much attention and criticism by judges in many jurisdictions. The old adage, “You can’t please all the people all of the time,” is particularly relevant here. Building consensus among judges about how the final form should be laid out on screen, what it would look like in printed form, where signature boxes would be, and so on has been a larger challenge than foreseen by many. As with overcoming resistance, early involvement of judges in the planning and development phases is important to identify format concerns and work towards a reasonable solution that would satisfy most. In Washington, the collaborative planning team focused on the benefits of the systems approach as a way to steer judges toward a common template.

There is one additional challenge that was not common to the jurisdictions studied, but deserves attention, nevertheless. In some states, like Georgia and Texas, part-time prosecutors may have a separate private practice in which they may represent defendants in DUI cases. This creates an issue with regard to the eWarrant process if prosecutors have access to search warrants. One potential solution is to create a policy which limits access to eWarrants to only those cases in which the individual is the lead prosecutor, or if the prosecutor's private practice is only able to take cases in jurisdictions he/she does not prosecute in, access can be limited to the prosecution jurisdiction.

UNINTENDED CONSEQUENCES

With eWarrant systems, unintended consequences range from impacting drug recognition expert (DRE) evaluations, resulting in a greater number of dismissals in drugged driving cases, to creation of significant delays in blood test results. The lessons learned in five jurisdictions studied by JMI, as well as information provided by the expert working group, provide insight into how to mitigate these unintended consequences.

Some jurisdictions have noted a decrease in DRE evaluations which seems to coincide with the implementation of eWarrants. With the implementation of eWarrant systems, law enforcement officers have confidence they can obtain a chemical sample from a suspect in an expeditious manner. As a result, there is increased reliance on the blood alcohol concentration being admitted as evidence in court. Similarly, the ease in acquiring a blood draw can lead to a false sense that any drug use will also be captured and admitted into evidence and it is no longer necessary to rely on a DRE's opinion. However, in instances where drug or polysubstance impairment is suspected it is imperative a DRE evaluation be performed if there is an officer available. Overreliance on blood testing to make a case instead of relying on extensive documentation of the signs and symptoms of impairment that are part of a DRE evaluation can result in a weaker case. It is well-established that the presence of a drug(s) within the body does not necessarily infer impairment at the time of driving and in states that do not have per se levels for these substances, the testimony of DREs is extremely valuable in articulating if and how an individual is impaired.

Further complicating this issue is the fact that in a number of jurisdictions' laboratories will not test blood for controlled substances if the initial blood alcohol content result is at or above .08. Unfortunately, many state labs are faced with testing backlogs and opt to prioritize testing based on resource levels. Additional analyses of samples in cases where a driver has an alcohol concentration above the legal limit is often viewed as an unnecessary use of lab and technician time/resources, if it is unlikely to affect the charging decision and/or case outcome (i.e., the individual can be prosecuted and convicted of DUI so it is less important to identify whether they were simultaneously under the influence of drugs at the time of driving). This practice results in the underrepresentation of drug and polysubstance-impaired driving in these jurisdictions and, subsequently, characteristics of the problem cannot be adequately quantified. Moreover, it diminishes the possibility of mandatory minimum sentencing in cases involving certain drugs.

Another drawback in this scenario is if DRE evaluations are not performed, there may be no findings to support polysubstance-impaired driving even if an officer assumes a blood test will provide sufficient evidence of drug use. The failure to admit evidence of drug impairment misses an opportunity to provide prosecutors and judges with valuable information that could ultimately affect decision-making. Further, failure to identify individuals who are polysubstance users has the potential to lead to poor supervision and treatment outcomes. Ideally, all underlying causes of offending will be identified, but this often is not the case. The additional information contained within DRE evaluations can help pinpoint those individuals who may need services beyond alcohol education and treatment.

To address this problem of officers forgoing the DRE evaluation, Utah has incorporated eWarrant training and the continued need for DRE evaluations into its DRE school to ensure not only officers, but also prosecutors and judges continue to recognize the value and merit of the DRE evaluation. In Virginia, to help ensure blood tests include alcohol and other controlled substances, prosecutors now specifically ask for the additional testing.

The impact on lab turnaround time is another unintended consequence experienced by nearly all the jurisdictions studied, with return times increasing from as little as 2-3 weeks to as much as 3-4 months or longer. Among the reasons for the longer return times noted by the expert working group were the increased volume of samples being submitted for testing as well as the requirement of technicians to testify in court, which reduces the amount of time they have available in the lab. Travel time, and time out of the laboratory to provide testimony, places a huge demand on lab resources, which can affect the lab's ability to conduct tests in a timely manner. To reduce the burden on the laboratories, Utah as well as other jurisdictions, have relied on the rules of criminal procedure, which allow for video testimony from experts. Wyoming allows this too, however, if the defendant exercises his/her right to confrontation, the expert must appear in-person at trial. Texas has addressed this by creating a waiver to file the affidavit in trial; if the defendant does not object within 3 weeks of the trial date, the video testimony is admissible. The Texas appellate court upheld that this video testimony is admissible, holding that defendants' rights to confrontation were not violated by the process.

As noted earlier, engagement of labs in the planning process can help identify what the potential delays in processing times might be and offer insight into how to reduce this burden by exploring different lab models. Changes in how tests are handled provides another option for reducing the impact on timeliness of test results. Virginia, for example, does batch testing. Several jurisdictions, such as Illinois and Florida, noted that the use of private labs can help alleviate the burden. In Illinois, police departments share the \$65,000 per year cost for contracting with private labs. Naples, Florida also contracts with a private lab, and if the defendant is found guilty, part of the sentence is a fee to allow for cost recovery. Under Chapter 59.06(d-2) of the Texas Code of Criminal Procedure, law enforcement can use forfeiture funds to pay for a private crime lab to analyze blood tests.

While it is not possible to foresee every potential challenge that will arise post-implementation, proper preparation and planning can minimize problems. The involvement of a diverse range of stakeholders at this phase is key to obtain a multitude of perspectives on how the eWarrant system could potentially affect decision-making and the ability of practitioners to perform their jobs. It is also recommended that those in charge of system development and implementation consult with outside agencies who have previously navigated this process. The lessons learned from other jurisdictions' experiences could prove quite valuable.

IMPROVING DUI SYSTEM EFFICIENCY

A Guide to Implementing Electronic Warrants

SECTION 9

Best Practices & Lessons Learned

SECTION 9:

Best Practices and Lessons Learned

Each of the jurisdictions studied by JMI, as well as those represented by the expert working group members, are prime examples of effective approaches to the implementation of eWarrants and eWarrant systems. To the extent a jurisdiction has the technological capacity and resources available, a fully-integrated system is recommended – one that supports both the preparation and transmission of the warrant, return of service, and links to criminal history and state drivers' licensing agencies. Regardless of whether a jurisdiction opts for implementing such a system or simply automates the warrant, there are a number of lessons learned that can be applied.

Based on the experiences of these jurisdictions and the characteristics of the systems ultimately developed, there are several key practices that are considered “best practice” and are recommended for any jurisdiction planning to implement or refine an existing eWarrant or eWarrant system. In the planning and design phase, the best practices are largely process-oriented. Individuals involved in the development of the most effective eWarrant systems shared the following strategies that ultimately laid the foundation for successful implementation:

- **Agency leadership** – identify the agency that will take the lead in the development and implementation of the eWarrant system. This agency will assume responsibility for coordinating efforts, convening stakeholders, and maintaining communication throughout the process. In this role, the agency should anticipate potential challenges and manage change, expectations, and any resistance.
- **Early and consistent stakeholder engagement** – identify and convene the right people as early in the process as possible. Stakeholders should not be limited to those in the lead agency or law enforcement; instead, input should be sought from a diverse range of individuals representing various facets of the DUI system. By being inclusive and engaging with traditional and non-traditional partners during the planning phase, agencies can better identify resources and challenges that will need to be overcome.

These individuals can also help identify and plan for any unintended consequences that implementation may cause. Communication with stakeholders should continue throughout the planning, development, and implementation phases to elicit feedback and obtain buy-in.

- **Identification of system needs** – determine what the new system will look like and how it will improve upon existing practice to guide system development. To accomplish this task, the lead agency should clearly state the problem to be solved and develop a series of goals and objectives. A high-level approach to preparation will allow the agency to make decisions based on thorough information-gathering.
- **Identification of funding sources** – develop a high-level estimate of costs for system development and implementation and include contingencies in the budget. If the system is to be used by multiple agencies, there may be shared costs and opportunities to reduce the financial burden on the lead agency. Various funding sources should be explored (e.g., state or grant funding, fees for cost recovery, and other creative solutions) to determine their viability.
- **Input from frontline users** – engage with individuals who will be using the system on a consistent basis to obtain their feedback on whether their needs and expectations will be met. While stakeholder perspectives should guide the planning and development phases, it is vitally important to also consider the views of those on the frontlines. In order for the technology to be accepted, it should be user-friendly and efficient for officers and judges. By including them in the process, additional challenges that may not have been considered can be identified and resistance to change can be overcome.
- **Pilot testing** – start small when rolling out any eWarrant system and pilot the technology with a single agency. This initial testing period provides an opportunity to build support for the new process/system and to address any user or technology issues before they create frustration. By pilot testing the system, agencies will also gain insight into training that will be needed to allow for expansion.



- **Consistent training** – develop comprehensive and consistent training to prepare users to seamlessly navigate the eWarrant system. There are multiple approaches to training that are commonly used including self-guided training; in-person training modules at law enforcement academies and DRE schools; presentations/workshops at statewide law enforcement and judicial conferences; and online help resources. Jurisdictions are encouraged to use the approach that will be best received among the target audience and to update content as necessary.
- **Use of device agnostic technology** – ensure that the technology chosen allows the user to access the eWarrant on different types of systems (e.g., Windows, Mac, Apple iOS, Android) and hardware (e.g., smartphone, tablet, laptop, or desktop computer); this also creates flexibility for adapting to new technologies as they emerge.

Another important lesson learned is that the creation of an eWarrant system should strive to streamline the entire warrant process – from preparation to approval to return of service. Many of the experts noted that inability to create an electronic process for the officer to swear to the facts, can limit the effectiveness and timeliness of the eWarrant processing. Those jurisdictions that were able to incorporate electronic oaths, using penalty of perjury statements or some other electronic means of swearing to the fact, experienced faster processing times than those in which in-person oaths were required. Jurisdictions should examine the feasibility of electronic oaths during the planning process as the ability to incorporate this into an eWarrant system may require legislative change.

Despite solid planning, implementation, and training, the process for legally obtaining blood tests in DUI cases is not infallible. One recent case, discussed in the sidebar, demonstrates the importance of officer oversight and system reviews, metrics that allow supervisors and administrators to track that appropriate procedures are followed, and continuous training/re-training of officers to ensure they have a clear understanding of operations, policies, procedures, and applicable law. In Utah, the state legislators went as far as introducing a bill that makes it clear that blood draws are only permitted with the person's consent, a warrant, or an explicit judicially recognized exception to a warrant. The bill will be considered by the full legislature in 2018.

IMPORTANCE OF CONSISTENCY & SUPERVISION

A recent case in Salt Lake City, Utah demonstrates the importance of consistency and supervision.

In July 2017, a crash victim was brought unconscious into the hospital, where the officer asked the nurse to collect a blood sample from the crash victim. The nurse refused, noting the victim was not under arrest and citing both hospital policy and Utah law recommending a warrant for a blood draw. The officer insisted he had implied consent to obtain the sample and arrested the nurse.

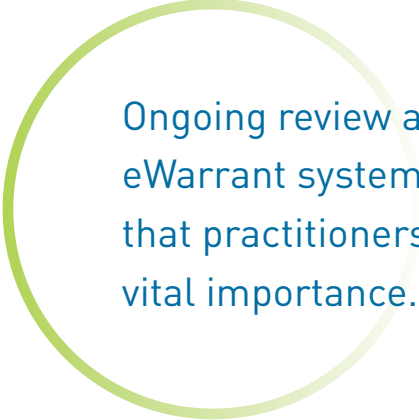
An internal review of the incident found that although the officer's intentions may have been just, he failed to use the training and tools provided that allow him to obtain BAC tests without violating policy or violating suspects' Constitutional rights. As a result of this incident, the Salt Lake Police Department has updated their blood draw policy to be consistent with hospital policy and re-trained officers on the updated policy and protocols.

Once designed, there are several key policies and operational practices that have demonstrated significant positive results in DUI enforcement and adjudication. These include the following:

- Checkboxes or prompts to ensure completeness and accuracy of information being submitted.
- Incorporation of pre-populated information for such items as:
 - Hero statement, that is prepared by the user when he/she sets up an account, and will automatically add the user's qualifications and training.
 - Driver's information, which allows an officer to initiate a search based on name and date of birth to confirm the identity of the suspect and auto-populate the demographic fields (address and driver's license information).

- Inclusion of open text fields to allow officers to add a narrative or observations as necessary.
- Automated judicial assignment based on the location the warrant is being requested (alternatively, several jurisdictions use a pull-down menu that shows available judges).
- Addition of a penalty of perjury statement on the warrant to allow for statements to be sworn in electronically or digitally as opposed to in-person.
- Inclusion of a pull-down menu of reasons for rejection if the warrant is denied, along with the option for text input, which not only allows the officer to see the reason for denial and potentially correct it, but also serves as a source of data for additional training if common mistakes are being made by officers.
- Real-time tracking and data analytics that allow officers and judges to see the warrant status and allow system administrators to run reports on system use and outcomes.

Lastly, ongoing review and updates to eWarrant systems is a practice that practitioners agree is of vital importance. As highlighted in [Section 6](#), assessment is needed to ensure that intended goals are being met and to identify areas for improvement. By capturing system analytics and tracking change over time, the benefits of the system can be quantified.



Ongoing review and updates to eWarrant systems is a practice that practitioners agree is of vital importance.

IMPROVING DUI SYSTEM EFFICIENCY

A Guide to Implementing Electronic Warrants

Conclusion

Conclusion

Although the process for designing and implementing eWarrants can be time-consuming and seemingly complex, the bottom line is that whatever system is adopted, it should be user-friendly and make the DUI arrest process more efficient. By following the steps outlined in this report, agencies can replicate the success experienced in other jurisdictions and learn from the challenges they faced. Through proper planning, stakeholder engagement, pilot testing, and training agencies can implement and expand eWarrant systems.

The demonstrable benefits of eWarrant systems including, reduced burden on law enforcement, faster DUI arrest processing, fewer errors and omissions resulting in denied requests for warrants, availability of more BAC test results, greater likelihood of conviction, better information for assessing offenders, and an enhanced deterrent effect on hardcore drunk drivers as well as the public at large, reveal that a well-thought out eWarrant system is of significant importance in the fight against impaired driving. By automating the warrant process, we give law enforcement officers a streamlined tool for pursuing justice and ensuring that individuals who drive impaired are held accountable.

By automating the warrant process, we give law enforcement officers a streamlined tool for pursuing justice and ensuring that individuals who drive impaired are held accountable.



References

References

Beck, K. (1999). Effects of ignition interlock license restrictions on drivers with multiple alcohol offenses: A random trial in Maryland. *American Journal of Public Health*, 89, 1696-1700.

Berkovich, E. (2015). Utah Improves DUI Test Submission Rate. *NAPC Newsbreak*, Fall(4).

Federal Bureau of Investigation (FBI). (2016). [Crime in the United States, 2016: Table 18, Estimated Number of Arrests, 2016](#).

Fell, J. (1995). Repeat DWI Offenders in the United States. [Traffic Tech, No. 85](#). Washington, DC: National Highway and Traffic Safety Administration.

Jewett, A. (2015, August 7). [Alcohol-impaired driving among adults - United States, 2012](#). *Morbidity and Mortality Weekly Report (MMWR)*, 64(30), 814-817.

Jones, R., & Lacey, J. (2000). [State of Knowledge of Alcohol-Impaired Driving: Research on Repeat DWI Offenders](#). Washington, DC: National Highway Traffic Safety Administration.

Maruschak, L. (1999). [DWI Offenders Under Correctional Supervision](#). NCJ 172212. Washington, DC: Bureau of Justice Statistics, U.S. Department of Justice.

NHTSA. (2017). Alcohol-impaired driving. [Traffic Safety Facts: 2016 Data](#). DOT HS 812 450. Washington, D.C.: National Highway Traffic Safety Administration.

NHTSA. (n.d.). [Risky Driving](#). Retrieved November 6, 2017, from National Highway and Traffic Safety Administration: <https://www.nhtsa.gov/risky-driving/drunk-driving>

Responsibility.org. (2016). [2015 State of Drunk Driving Fatalities in America](#). Arlington, VA: Author.

Responsibility.org. (n.d.). [Get the Facts](#). Retrieved November 6, 2017, from Responsibility.org: <https://www.responsibility.org/get-the-facts/>

Robertson, R., & Simpson, H. (2002). *DWI System Improvements for Dealing with Hard Core Drinking Drivers: Adjudication and Sanctioning*. Ottawa: Traffic Injury Research Foundation.

Siegal, H., Falck, R., Carlson, R., Rapp, R., Wang, J., & Cole, P. (2000). The hardcore drunk driving offender. *Proceedings of the 15th International Conference on Alcohol, Drugs, and Traffic Safety*. Stockholm, Sweden. Retrieved November 8, 2017, from http://www.icadtsinternational.com/files/documents/2000_025.pdf



IMPROVING DUI SYSTEM EFFICIENCY

A Guide to Implementing Electronic Warrants

APPENDIX A

Expert Working Group Members & Reviewers

APPENDIX A:

Expert Working Group Members & Reviewers

Peggy Bell, Executive Director

Delaware Criminal Justice Information System
802 Silver Lake Blvd, Suite 101
Dover, DE 19904

Peggy.Bell@state.de.us

Chuck Hayes, Program Manager

Drug Evaluation and Classification Program
International Association of Chiefs of Police
44 Canal Center Plaza, Suite 200
Alexandria, VA 22314

hayes@theiacp.org

Vernon F. Betkey, Jr., Manager

National Law Enforcement Liaison Program
Governors Highway Safety Association
444 North Capitol Street NW, Suite 722
Washington, DC 20001

vbetkey@ghsa.org

Erin Holmes, Director of Traffic Safety

Foundation for Advancing Alcohol Responsibility
2345 Crystal Dr., Suite 710
Arlington, VA 22202

erin.holmes@responsibility.org

M. Kimberly Brown, Senior Attorney

National Traffic Law Center
National District Attorneys Association
1400 Crystal Drive, Suite 330
Arlington, VA 22202

mkbrown@ndaajjustice.org

Edward Hutchison, Director

Triad, Traffic and Officer Safety
Staff Liaison, Drug Enforcement, Traffic Safety
National Sheriffs' Association
1450 Duke Street
Alexandria, VA 22314

ehutchison@sheriffs.org

Detective Brett N. Campbell, Drug Recognition Expert

City of Phoenix Police Department
Vehicular Crimes Unit
620 West Washington Street
Phoenix, AZ 85003

brett.campbell@phoenix.gov

Trooper Jason Marshall**State Drug Recognition Expert Coordinator**

Utah Highway Patrol
410 West. 9800 South
Sandy, UT 84070

jmarshall@utah.gov

Petey Casstevens, Consultant

Foundation for Advancing Alcohol Responsibility

casstevensp@gmail.com

Russ Martin, Director, Government Relations

Governors Highway Safety Association
444 N. Capitol Street, NW Suite 722
Washington, DC 20001

rmartin@ghsa.org

Steven Casstevens, Chief of Police

Buffalo Grove Police Department
46 Raupp Boulevard
Buffalo Grove, IL 60089

scasstevens@vbg.org

Brandy Nannini, Vice President, Government Relations & Traffic Safety

Foundation for Advancing Alcohol Responsibility
2345 Crystal Dr., Suite 710
Arlington, VA 22202

brandy.nannini@responsibility.org

Jennifer Cifaldi, Traffic Safety Resource Prosecutor

Institute for Legal, Legislative, and Policy Studies
 University of Illinois Springfield
 Center for State Policy and Leadership
 One University Plaza, MS PAC 451
 Springfield, IL 62703
jcifaldi3@gmail.com

Ashley Schluck, Traffic Safety Resource Prosecutor

Wyoming Highway Safety
 City of Laramie Attorney's Office
 P.O. Box C
 Laramie, WY 82073
aschluck@cityoflaramie.org

Kyle Clark, Project Manager

Drug Evaluation and Classification Program
 International Association of Chiefs of Police
 44 Canal Center Plaza, Suite 200
 Alexandria, VA 22314
ClarkK@theiacp.org

Ken Stecker, Traffic Safety Resource Prosecutor

Prosecuting Attorneys Association of Michigan
 58800 S. Burr Oak Road
 Colon, MI 49040
steckerk@michigan.gov

Warren Diepraam, Consulting Attorney

Looney & Conrad, P. C.
 645 12th Street
 Hempstead, TX 77445
wkdiepraam@yahoo.com

Stephen K. Talpins, Chairman of the Board

National Partnership on Alcohol Misuse and Crime
 12828 Equestrian Trail
 Davie, FL 33330
sktalpins@aol.com

Lt. Michael Edgar, DECP/SFST State Coordinator

OIC Applied Technology Unit
 Louisiana State Police Training Academy
 901 Independence Boulevard
 Baton Rouge, LA 70806
Michael.Edgar@la.gov

Kent Therkelsen, Product Manager

Bureau of Criminal Apprehension
 1430 Maryland Avenue East
 St. Paul, MN 55106
kent.therkelsen@state.mn.us

Sean Fitzpatrick, Traffic Safety Coordinator

National Sheriffs' Association
 1450 Duke Street
 Alexandria, VA 22314
sfitzpatrick@sheriffs.org

Joanne Thomka, Program Attorney

National Association of Attorneys General
 1850 M Street NW, 12th floor
 Washington DC 20036
jthomka@naag.org

Darrin T. Grondel, Director

Washington Traffic Safety Commission
 PO Box 40944
 Olympia, WA 98504
dgrondel@wtsc.wa.gov

**Sergeant Seth Weinstein,
Special Operations Team Leader**

Alexandria Police Department
 301 King Street
 Alexandria, VA 22314
Seth.Weinstein@alexandriava.gov

**A Guide to Implementing
Electronic Warrants**

APPENDIX B

Legislative Matrix

APPENDIX B:

Legislative Matrix



NATIONAL DISTRICT ATTORNEYS ASSOCIATION NATIONAL TRAFFIC LAW CENTER Telephone, Video, and Electronic Search Warrants

States where search warrants may be issued on the basis of telephonic, video or electronic affidavits:

STATE	RULE/STATUTE AND OPERATIVE LANGUAGE
-------	-------------------------------------

AL	Ala. R. Crim. P. Rule 3.8: "If circumstances make it reasonable to dispense...with a written affidavit" a warrant may be issued "based upon sworn testimony communicated by telephone or other appropriate means, including facsimile transmission"; requesting person prepares a duplicate document and reads it to the magistrate, who creates "the original warrant"; the applicant is directed to sign the magistrate's name to the duplicate; magistrate is to place caller under oath and If recording device is available, record the exchange; otherwise make written record; also, the magistrate may direct that the proposed warrant be modified
AK	Alaska Stat. § 12.35.010: warrant "may issue upon the sworn oral testimony...communicated by telephone or other appropriate means, or sworn affidavit submitted by facsimile" Alaska Stat. § 12.35.015: applicants to be placed under oath and a voice recording device to be used; duplicate warrant to be prepared if facsimile cannot be transmitted; applicant to sign the judicial officer's name on the warrant and judicial officer signs the original warrant; also, the magistrate may direct that the duplicate original warrant be modified
AZ	A.R.S. §13-3914: "In lieu of, or in addition to, a written affidavit...the magistrate may take an oral statement under oath which shall be recorded...(and which)...may be given in person to the magistrate or by telephone, radio, or other means of electronic communication A.R.S. §13-3915: if the applicant for the warrant "is not in the actual physical presence of the magistrate" the applicant may be authorized to sign the magistrate's name to a "duplicate original warrant"; the magistrate signs the original warrant and files both when the duplicate is returned; the magistrate's signature may also be affixed on "a telefacsimile of an original warrant"
AR	A.C.A. §16-82-201: "If the circumstances make it reasonable to dispense with a written affidavit" a warrant may be issued based upon "sworn oral testimony communicated by telephone or other appropriate means"; applicant to prepare duplicate warrant and to be directed to sign the judicial officer's name ; applicant to be placed under oath and recording to be made if device is available; if longhand verbatim record is made, the judicial officer is to file a signed copy; also, the judicial officer may direct that the warrant be modified Ark.R.Crim.P. Rule 13.1: application and affidavit may be submitted facsimile "or by other electronic means"; if oral testimony, judicial officer to place applicant under oath and "recorded testimony" may be received; judicial officer signs warrant and then transmits by facsimile or other electronic means

CA **Cal Pen Code §1526:** if the oath is made “using telephone and facsimile transmission equipment, telephone and email, or telephone and computer server” the affiant transmits the affidavit and proposed warrant to the magistrate, who confirms receipt, verifies that all pages are received and that affiant’s signature (which may be original, digital, or electronic) is genuine; magistrate notes that a telephone oath was administered, signs the warrant and transmits it; this is now deemed the “original” warrant

CO **C.R.S. 16-1-106:** written applications and affidavits and warrants may be submitted and issued “by an electronically or electromagnetically transmitted facsimile or by an electronic transfer that may include an electronic signature”; these documents are to be treated as original documents

Colo.Crim.P. 41: warrants, signed affidavits and accompanying documents “may be transmitted by electronic facsimile transmission (fax) or by electronic transfer with electronic signatures” and judges may treat these documents as originals; a warrant affidavit “may be sworn to or affirmed” by oath administered over the telephone

DC **D.C. Code §23-522:** “Each application for a search warrant shall be made in writing, or by telephone or other appropriate means, including facsimile transmissions or other electronic communications, upon oath or affirmation to a judicial officer”

D.C. SCR-Crim. Rule 4.1: “A judge may consider information communicated by telephone or other reliable electronic means” if the applicant/affiant is placed under oath and examined, a record is created, and original and duplicate documents are prepared; if documents are transmitted to the judge “by reliable electronic means, the transmission received by the judge may serve as the original”; also, the judge may modify the warrant and if so, transmit the modified version to the applicant or direct the applicant to modify the “proposed original warrant” and file the modified original warrant as modified by the judge

FL **Fla. Stat. §933.07:** A judge may electronically sign a search warrant if satisfied that probable cause exists and the judge determines that the affiant’s signature or electronic signature is present, that the application is supported by oath administered “by the judge or other person authorized by law to administer oaths” and that if the documents were submitted electronically, the submission was “by reliable electronic means”; the warrant is deemed issued when the judge’s signature or electronic signature is affixed

GA **O.C.G.A. §17-5-21.1:** Search warrants may be issued “by video conference” provided that when a judge issues such a warrant, the judge is physically located in the state; the judge shall administer an oath to any person testifying; a video recording shall be submitted and maintained as part of the record, and the judge and the affiant shall sign their respective documents “by any reasonable means” by which they can be identified, including but not limited to a “type-written name, signature affixed by electronic stylus, or any other reasonable means”

HI **Haw. R. Penal P. Rule 41:** “[a] warrant shall issue only on an affidavit or affidavits sworn to before the judge...”; however, “a sworn oral statement, in person or by telephone, may be received”, recorded and transcribed, and in such cases, this statement is deemed to be an affidavit; a judge may orally authorize an officer to place the judge’s “signature” on a duplicate original warrant, “which shall be deemed to be a valid search warrant...”

-
- ID** **Idaho Code** §19-4404: in lieu of a written affidavit, a judge may administer oaths by telephone and take testimony by telephone; oral testimony “as recorded” must be filed with the clerk
- Idaho Code** §19-4406: if the affidavit is “related to the court telephonically” the officer may be authorized to sign the magistrate’s name on a “duplicate original warrant” which must then be returned to the magistrate, who then “shall endorse his name and enter the date on the warrant when it is returned to him”
- Idaho Code** §19-4408: service may be made “in person, by mail or facsimile transmission, or by electronic mail. Unless an investigation necessitates otherwise, the officer should attempt notification on the person whom it is served prior to electronic mail service”
- I.C.R. 41:** court rule providing for receipt of information “communicated by telephone or other reliable electronic means” and for sending a copy of a warrant electronically to an officer for service of the warrant
-
- IL** **725 ILCS 5/108-4:** a warrant upon written complaint may be issued “electronically or electromagnetically by use of electronic mail or a facsimile transmission machine”; in terrorism or terrorism-related cases, a warrant upon oral testimony may be used, when circumstances make it reasonable to dispense with a written affidavit; in other cases, a warrant may be issued “upon testimony by simultaneous video and audio transmission”; if possible, the requestor should submit material to the judge by facsimile, email, “or other reliable electronic means”; if that is or if impracticable, the requestor is to read a proposed warrant to the judge who then makes a verbatim copy; the oath and all testimony to be recorded; these warrants are warrants of the issuing judge and not of the court, so no court seal need be placed on the warrant; also, the judge may direct that the warrant be modified
-
- IN** **Burns Ind. Code Ann.** §35-33-5-8: a judge may issue a search warrant without an affidavit if the judge receives testimony subject to the penalties for perjury of the same facts required for an affidavit “in a nonadversarial, recorded hearing before the judge; orally by telephone or radio; in writing by facsimile transmission (FAX); or in writing by electronic mail or other electronic communication”; statute provides special rules for each of the alternatives and provides that electronic signatures may be used for the affiant or the judge; also, the judge may direct the applicant to modify the warrant or may modify a transmitted warrant and transmit that modified warrant to the applicant
-
- IA** **Iowa Code** §321J.10: telephone warrants may be used after a refusal to test in a DUI case in which the DUI caused death or serious injury; procedure includes placing the caller under oath, the magistrate preparing a verbatim copy, use of a duplicate warrant for service and “if a recording device is available” recording the call and ultimately transcribing it
- Iowa Code** §462A.14D: telephone warrants after a refusal to test in a boating while intoxicated case causing death or serious injury; procedure similar to DUI warrants (in both this statute and the DUI statute, the magistrate may direct that the warrant be modified)
- Iowa Code Chapter 808:** legislative changes effective July 1, 2017 permit electronic submission of search warrant documents, telephone testimony, and electronic issuance of search warrants; the judicial branch to establish “processes and procedures” for implementation
-
- KS** **K.S.A.** §22-2502: warrants may issue on oral or written statements “conveyed or received by electronic communication” oral statements are to be “reduced to writing as soon thereafter as possible”
- K.S.A.** §22-2504: “warrants may be transmitted by electronic communication”

KY **KRS §455.170:** “The Supreme Court of Kentucky may, by rule, authorize a process allowing a search warrant to be applied for and issued electronically...”

LA **La. C.Cr.P. Art 162:** an affidavit containing the electronic signature of the applicant will suffice “provided that such signature is made under penalty of perjury...”

La. C.Cr.P. Art 162.1: sworn oral testimony may be communicated “by telephone, radio, or such other electronic method of communication deemed appropriate by the judge”; a recording shall be made and then “transcribed and fixed in the record within seven days”; there is also a provision for testimony by facsimile “after the administration of the oath by the judge by telephone, radio, or other such electronic method...”

ME **15 M.R.S. §55:** “The Supreme Judicial Court shall by rule provide the procedure of the application for and issuance of search warrants.”

Me. R. U. Crim. P. Rule 41C: a request for a search warrant made from outside the presence of the court “must be in the form of a written affidavit transmitted by reliable electronic means”; the applicant, “by telephone or other electronic means” must attest to its contents; the court may hear evidence under oath or affirmation “by telephone or other reliable means” and have that taken down by court reporter or recorded; a proposed search warrant transmitted to the court may serve as the original; if signed the court transmits the warrant “by electronic means” to the applicant, and a copy of the warrant shall be promptly filed; also, the court may modify the proposed search warrant, and the issued warrant shall be filed

MD **Md. CRIMINAL PROCEDURE Code Ann. §1-203:** application is to be in writing and may be submitted “by secure fax” or “by secure electronic mail” if complete and printable images of all documents are submitted; the applicant may converse with the judge in person, or via telephone or video; the judge may sign and transmit the warrant and supporting documents by secure fax or by secure electronic mail

Md. Rule 4-601: applicant may transmit application, affidavit, and proposed warrant in person or “by secure facsimile” or “by secure and reliable electronic mail that permits the judge to print the complete text of the documents”; the warrant may be issued electronically

MI **MCLS §780.651:** affidavit “may be made by any electronic or electromagnetic means of communication, including by facsimile or over a computer network” if the judge orally administers an oath or affirmation to the applicant, and the applicant signs the affidavit (the signature may be on the affidavit before it is transmitted by facsimile, or an electronic signature on the affidavit “transmitted over a computer network”); warrant may be issued by facsimile or by any electronic or electromagnetic means of communication, and judge may sign an electronically issued warrant from any location in the state; an oath or affirmation administered by electronic means “is considered to be administered before the judge”; the transmitted copies of documents are “duplicate originals” not required to have an impression made by an impression seal

MCLS §780.651: statute addresses the validity of an oath or affirmation “administered by electronic or electromagnetic means of communication”

MN **Minn. R. Crim. P. 33.05:** warrants and other documents may be sent via electronic submission and such documents are “valid and enforceable”

Minn. R. Crim. P. 36.01-36.08: request for search warrant may be made , in whole or in part, on sworn oral testimony “via telephone, radio, or other similar means of communication” and “written submissions may be presented by facsimile or electronic transmission, or by other appropriate means”; the officer prepares a duplicate original warrant and reads it to the judge, who records, verbatim, what has been read (unless the judge permits the document to be transmitted to the judge); the proceeding must be recorded by the judge or, if the judge permits, by the officer requesting the warrant (who then must submit the recording to the judge as soon as practical); the judge may sign the warrant and transmit it to the officer or may direct that the officer sign the judge’s name to the duplicate warrant; all documents (including transcripts or a longhand verbatim record) to be filed; also, the judge may direct modifications, “which must be included on the original and any duplicate original warrant”

Minn. R. Crim. P. 37.01-37.02: search warrant applications must be supported by written affidavit, sworn to under oath or by written statement signed under penalty of perjury; if a judge administers an oath via telephone, radio, or similar means of communication and the applicant does no more than attest to the contents of a signed statement that was transmitted electronically, a verbatim recording of the oath is not required

MO **§542.276 R.S.Mo.:** application for search warrant “may be submitted by facsimile or other electronic means”

MT **46-5-222, MCA:** when an applicant seeks a search warrant by telephone, the applicant must “state reasons to justify immediate issuance”; the judge may administer an oath or affirmation by telephone, and the testimony must be subscribed the applicant and “attached to or logically associated with” the applicant’s electronic signature; a recording must be made by either the judge or the officer, and in either case, it must be transcribed verbatim as soon as possible; if the warrant is approved over the phone, the officer shall sign the warrant in the officer’s name and in the name of the judge, and if the judge signs the warrant by electronic signature, the peace officer must initial the judge’s signature and the officer’s signature “to indicate that the signatures were made electronically in accordance with this section”

NE **R.R.S. Neb. §29-814.01** an affidavit “may be submitted to the magistrate or judge in person or by facsimile or other electronic means and the warrant may be issued to the affiant in person or by facsimile or other electronic means”; if an officer wishes to request a warrant by telephone, the officer first contacts “the county attorney or a deputy county attorney...for purposes of explaining why a search warrant is to be issued pursuant to a telephonic statement”; if the prosecutor is satisfied that a warrant is justified and that circumstances justify its immediate issuance, the prosecutor is to contact the magistrate, provide the magistrate with a number where the officer may be reached, and then the magistrate “shall call the officer at the number provided and shall place the officer under oath and take his or her statement”; the magistrate must record the statement and a certified transcription is to be filed

R.R.S. Neb. §29-814.05: officer to complete a duplicate warrant and sign the judge’s name and the officer’s name to the warrant; the judge to complete and sign the original warrant and when the duplicate is returned, the judge is to sign the duplicate and both the duplicate and the original are then to be filed; if the judge fails to sign the duplicate, the warrant “shall be invalid”

Neb. Ct. R. §6-612 fax transmission authorized for warrants, and “a faxed document shall have the same force and effect as the original document issued by a court”

-
- NV** **Nev. Rev. Stat. Ann. §179.045:** “Secure electronic transmission may be used for the submission of an application and affidavit...and for the issuance of a search warrant by a magistrate”; “secure electronic transmission” is one by which only the intended recipient receives the information, the identity of the sender can be authenticated, and the information received is identical to the information that was sent
-
- NH** **RSA 595-A:4-a:** “The personal appearance and authorization for a search warrant under ...(the search warrant statute, RSA 595-A:4)...may be by means of telecommunication or electronic communication, and electronic signature...”
-
- NJ** **N.J. Court Rules, R. 3:5-3:** a Superior Court judge may issue a search warrant upon sworn oral testimony communicated by telephone, radio “or other means of electronic communication”; testimony shall be recorded or judge is to make longhand notes; the sworn testimony is deemed an affidavit, and if the judge is satisfied that “exigent circumstances exist to excuse the failure to obtain a written warrant” and sufficient grounds have been shown, the judge issuing the warrant directs the applicant to “enter this authorization verbatim on a form...designated as the duplicate original search warrant”; the judge also contemporaneously records the factual determination as to the exigent circumstances which justified the use of this procedure
-
- NM** **5-211 NMRA:** a request for a warrant may be made “by transmission of the affidavit and proposed search warrant...to the judge by telephone, facsimile, electronic mail, or other reliable electronic means”; judge may require appearance “personally, telephonically, or by audio-video transmission”; if the judge administers an oath “remotely” the means used must be designed to ensure that the judge confirms the identity of anyone testifying; the warrant “shall be transmitted by reliable electronic means” and the judge is to file a duplicate original with the court; signatures may be by original signature, by copy of an original signature, by a computer generated signature or “any other signature otherwise authorized by law”
-
- NY** **NY CLS CPL §690.35:** application may be in writing or oral
- NY CLS CPL §690.36:** oral applications may be by telephone, radio or other means of electronic communication; applicant must be identified and sworn, and other persons may testify if properly identified and sworn; oaths to be recorded by recording device, stenographer, or by longhand notes and transcription filed within 24 hours of issuance
- NY CLS CPL §690.40:** applicant to prepare warrant and read it, verbatim, to the judge
- NY CLS CPL §690.45:** warrants obtained on oral application must include the name of the issuing judge but not the judge’s “subscription”
-
- NC** **N.C.Gen.Stat. §15A-245:** written affidavit or “oral testimony under oath or affirmation presented by a sworn law enforcement officer...by means of an audio and video transmission in which both parties can see and hear each other” may support a warrant; to be considered, oral testimony must be “either recorded or contemporaneously summarized in the record or on the face of the warrant by the issuing official”

ND **N.D.R. Crim. P. Rule 4.1:** the magistrate may consider information communicated by telephone or other reliable electronic means; testifying persons must be placed under oath; the magistrate must record the testimony by a recording device, a court reporter, or in writing, and must certify and file the written record and exhibits; if the magistrate relies upon a sworn written affidavit, “the magistrate must acknowledge the attestation in writing on the affidavit”; the applicant must prepare a proposed duplicate and read its contents verbatim to the magistrate, who must enter the contents onto the original warrant; if the contents were transmitted “by reliable electronic means, the transmission received by the magistrate may serve as the original”; the magistrate must sign the original and transmit it, or direct the applicant to sign the magistrate’s name and enter the date and time on the duplicate original; also, the magistrate may modify the warrant and then transmit the modified version to the applicant or file the original modified version and direct the applicant to “modify the proposed duplicate original accordingly”

OH **Ohio Crim. R. 41:** if a search warrant affidavit “is provided by reliable electronic means, the applicant communicating the affidavit shall be placed under oath and shall swear or affirm the affidavit communicated”; if probable cause exists, “the warrant may be issued through reliable electronic means”

OK **22 Okl.St. §1223.1:** a magistrate may take an oral statement under oath “which shall at that time be recorded electronically and thereafter transcribed by an official court reporter” which then is deemed to be an affidavit and which is to be kept with the official records

22 Okl.St. §1225: an affidavit, proposed search warrant, or both “may be communicated to the magistrate by telephone or by electronic mail or any similar electronic communication which delivers a complete printable image of the warrant or affidavit”; the affiant is to recite the information establishing probable cause, recite the proposed warrant, and obtain the magistrate’s permission to place the magistrate’s name on the warrant; the magistrate’s oral recorded authorization to print the name “shall constitute issuance of the search warrant”; if electronic mail or other electronic communication is used, the affidavit may be sworn to by telephone and the magistrate may physically sign a printed copy and transmit it back to the affiant or return a copy of the document (as received or as modified by the magistrate) to the affiant; the magistrate may modify the warrant, “provided a copy of the modified document is included with the return electronic communication to the affiant”

OR **ORS §133.545:** instead of a written application, a judge make take an oral statement under oath, which shall be recorded and “the recording shall constitute an affidavit for the purposes of this section”; a written application may be a proposed warrant and affidavit sent to the court by facsimile transmission “or any similar electronic transmission that delivers a complete printable image of the signed affidavit and proposed warrant”; the affidavit may have a notarized acknowledgment or the affiant may swear to the affidavit by telephone; if an oath is sworn telephonically, the judge “must execute a declaration that recites the manner and time of the oath’s administration” which must be filed with the return; a signed warrant may be delivered to the person making the application by facsimile or similar electronic transmission; the original warrant is to be filed by the judge and the original affidavit is to be filed by the person making the application

PA **Pa. R. Crim. P. 203:** the “issuing authority” may use “advanced communication technology”; if such technology is to be used, the affiant must personally communicate with the issuing authority by any device “which, at a minimum, allows for simultaneous audio-visual communication” to permit verification of identity and oral administration of an oath; when a warrant is issued, “the issuing authority shall provide the original search warrant to the affiant and the issuing authority shall retain a contemporaneously prepared copy”

SC **Order of the Chief Justice of the Supreme Court of South Carolina (July 26, 2001):** Facsimile warrants permitted in extraordinary circumstances or after normal court hours; officer to “fully prepare the search warrant and all related affidavits”; officer then to call the appropriate magistrate, brief the magistrate on the need for the warrant, sign all of the pages of the warrant, and then fax the warrant to the magistrate. If the magistrate is satisfied with the warrant, the magistrate will call the officer and telephonically swear the officer to the facts contained in the warrant; the magistrate will then sign each page of the warrant and fax it back to the officer. The magistrate must confirm the identity of the officer by either voice identification, by contacting the dispatcher of the officer’s department for confirmation of the officer’s identity and confirmation that the officer is on duty and that the dispatcher or the officer’s supervisor is aware of the warrant request, or through use of a pager confirmation system

SD **S.D. Codified Laws §23A-35-4.2:** magistrate may receive an affidavit by electronic transmission and may issue a warrant by the same method; all applicable requirements for the issuance of a warrant shall be met, and the electronic document shall have the same force and effect as the original

S.D. Codified Laws §23A-35-5 (Rule 41(c)(2)): when circumstances make it reasonable, a search warrant may be issued upon sworn oral testimony communicated by telephone “or other appropriate means” which shall be recorded, transcribed, certified by the magistrate and filed with the court and which “shall be deemed to be an affidavit”

S.D. Codified Laws §23A-35-6 (Rule 41(c)(2)(A)): the applicant for a warrant must read verbatim the contents of the warrant and if approved, the magistrate shall direct the applicant to sign the magistrate’s name on the warrant; this is a duplicate original warrant “and is a warrant for purposes of this chapter”; the magistrate may direct that specific modifications be made, and in cases where the magistrate directs the applicant to sign the magistrate’s name, “the magistrate will have an original warrant made”

TN **Tenn. R. Crim. P. Rule 41:** a magistrate may issue a warrant based on information communicated by telephone or other reliable electronic means; the proposed warrant, the affidavit and supporting documents may be transmitted by facsimile transmission or by electronic transfer to the magistrate; the warrant affidavit shall be sworn to using audio-visual means; the documents received by the magistrate shall be deemed originals and filed with the clerk of court and the magistrate shall issue a copy of the warrant, with electronic signatures, to the affiant; “this section does not alter the requirement that the affidavit be submitted to the magistrate in writing regardless of the means of transmission”

TX **Tex. Code Crim. Proc. Art. 18.01:** a magistrate may consider information communicated “by telephone or other reliable electronic means”; a person providing testimony must be placed under oath; if an affidavit is submitted by reliable electronic means, “the magistrate must acknowledge the attestation in writing on the affidavit; if additional testimony is considered, the testimony must be recorded verbatim by recording, by court reporter, or by writing, this must then be transcribed, and all documents are to be certified as accurate and preserved; the applicant must prepare a duplicate original warrant, and read the contents verbatim or transmit the contents; the magistrate may modify the submitted warrant and if so, may transmit a modified warrant or direct the applicant to modify the duplicate warrant; the magistrate must sign the original documents and transmit them to the applicant, or direct the applicant to sign the magistrate’s name on the duplicate original

UT **Utah R. Crim. P. Rule 40:** “remotely communicated warrants” may be issued “when reasonable under the circumstances”; a request to the magistrate may be made by “voice, image, text, or any combination of those, or by other means”; testimony is to be under oath and recorded, which may be “by writing or by mechanical, magnetic, electronic, photographic storage, or by other means”; the magistrate may direct the applicant to sign the magistrate’s name, and the warrant and recorded testimony shall be retained and filed with the court

VT **V.R.Crim.P. Rule 41:** a warrant may be issued based on information “communicated by reliable electronic means” (which includes facsimile, electronic mail or “other method of transmitting a duplicate of an original document”); the applicant notifies a judicial officer that a signed or unsigned affidavit will be transmitted; an oath is to be administered over the telephone and noted on the affidavit; “the determination of probable cause ...shall be made solely on the contents of the affidavit or affidavits provided”; the applicant prepares and submits an original warrant and the judicial officer may sign (or modify and then sign) the warrant, and return a copy to the applicant; the judicial officer then enters the signed original (or modified) warrant into the record

VA **Va.Code Ann. §19.2-54:** the affidavit “may be filed by electronically transmitted (i) facsimile process or (ii) electronic record”; the affidavit is to be certified by the officer who issues the warrant and transmitted or delivered to the clerk; “‘affidavit’ ...means statements made under oath or affirmation and preserved verbatim”

WA **Rev.Code Wash. (ARCW) §10.79.035:** search warrant applications “may be provided or transmitted to the magistrate by telephone, email, or any other reliable method”

Wash. CRR 2.3: evidence in support of the warrant must be in the form of affidavits, “or sworn testimony establishing the grounds...and may be provided to the court by any reliable means. Any sworn testimony must be recorded and made part of the court record and shall be transcribed if requested”; the court “shall issue a warrant or direct an individual whom it authorizes for such purpose to affix the court’s signature...the court’s authorization may be communicated by any reliable means”

WI **Wis.Stat. §968.12:** search warrant may be based upon sworn testimony “communicated to the judge by telephone, radio, or other means of electronic communication”; requester prepares a duplicate original warrant and reads it, verbatim, to the judge, who enters what is read on the original warrant; when issuing the warrant, the judge directs the person requesting the warrant to sign the judge’s name on the duplicate original warrant and the judge signs the original warrant; the requester may send a proposed warrant by electronic transmission and the judge may sign that document and transmit that signed warrant to the requester; a caller will be placed under oath and any necessary testimony will be under oath, recorded, and ultimately transcribed and filed with the court; also, the judge may direct that the warrant be modified

WY **Wyo.Stat. §31-6-102:** if a DUI defendant has caused a serious injury or death and refuses testing, an officer or a prosecuting attorney may seek “a remotely communicated search warrant, when reasonable under the circumstances”; in such cases, all communication between the judicial officer and the requestor “may be remotely transmitted by voice, image, text or any combination thereof, or by other means and shall be recorded...by writing or mechanical, magnetic, electronic, photographic storage or by other means”; the judicial officer may direct the requestor to sign the judicial officer’s name “on a warrant at a remote location”

W.R.Cr.P. Rule 41: search warrants may be based “wholly or partially” on recorded sworn testimony, preserved by a court reporter or by a recording device; if the judicial officer is to issue a warrant based upon communication received by “telephone or other electronic means” and if a telephone warrant is used, the requestor and any witnesses must be placed under oath; the requestor must prepare a proposed duplicate warrant, and the judicial officer must enter the contents of the proposed duplicate warrant into an original warrant; the judicial officer may direct that the warrant be modified; if the proposed duplicate warrant is received by electronic means, the judicial officer may modify it (in which case it can serve as the original warrant), and then transmit the original warrant (or the modified warrant) to the requestor

IMPROVING DUI SYSTEM EFFICIENCY

A Guide to Implementing Electronic Warrants

APPENDIX C

Business Process Analysis Resources

APPENDIX C:

Business Process Analysis Resources

Business Requirements Document Sample (including workflow diagrams and document indices)

The following sample business requirements document is for the design and implementation of an e-Filing application. It is provided for illustrative purposes only as the scope for the design and implementation of an eWarrant system will necessarily be different. Also included in this BRD are sample workflow diagrams and document indices.



3.0 E-Filing Application

[Click to view](#)

Requirements Traceability Matrix Sample/Template

Requirements Traceability Matrix Sample/Template

NOTE: THE FOLLOWING REQUIREMENTS TRACEABILITY MATRIX IS DRAWN FROM A REQUEST FOR PROPOSALS FOR AN NEW INFORMATION SYSTEM. AS PART OF THE PROCESS FOR DESIGNING THE EWARRANT SYSTEMS, JURISDICTIONS WOULD COMPLETE THIS INFORMATION UNLESS A VENDOR IS HIRED TO CONDUCT THE BUSINESS PROCESS ANALYSIS.

The Global and Functional Specifications checklists below identify desired functions and features of the Franklin County Juvenile Justice Information System (JJIS), a unified relational database which is accessed by the various units of the Juvenile Court for case initiation, management, assignment, monitoring, reporting notification and administration. The JJIS scope does not include the Franklin County Clerk of Court's Justice System (FCJS), but many reports and case events relating to the juvenile may eventually be docketed to the FCJS or require access to data maintained in the FCJS. Development of the system is intended to have a standalone system which will be operated by the Franklin County Clerk of Court.



Requirements Traceability Matrix Sample/Template

Completion of the Global and Functional Specifications Checklists contained in the section is mandatory. The specifications include functional and technical requirements for the proposed JJIS application seen in the following categories:

[Click to view](#)

- **Global Specifications:** General administrative and technical specifications which apply globally across the proposed application and must be met for all units, modules and functionality. This includes but is not limited to security, application tables, application reporting, and document and user administration.
 - *Note: Documentation on the overall technical requirements, current user counts, organization charts and other data relevant to the global specifications are contained elsewhere in this RFP.*
- **Intake and Diversion Unit:** Functional requirements necessary to complete the operational, reporting, administration, and noticing requirements of the Intake and Diversion Unit.
- **Probation:** Functional requirements necessary to complete the operational, reporting, administration, and noticing requirements of the Probation Unit including Care Coordination, Pre-Sentence Investigation, Alternative to

IMPROVING DUI SYSTEM EFFICIENCY

A Guide to Implementing Electronic Warrants

APPENDIX D

Sample RFP

APPENDIX D:

Sample RFP from Washington State Patrol

Unless an electronic warrant system is developed in-house, agencies will need to contract for services. To access an example of a Request for Proposal (RFP) that was issued by the Washington State Patrol, click on the image below.



Washington State Patrol Information Technology Division

[Click to view](#)



IMPROVING DUI SYSTEM EFFICIENCY

A Guide to Implementing Electronic Warrants

APPENDIX E

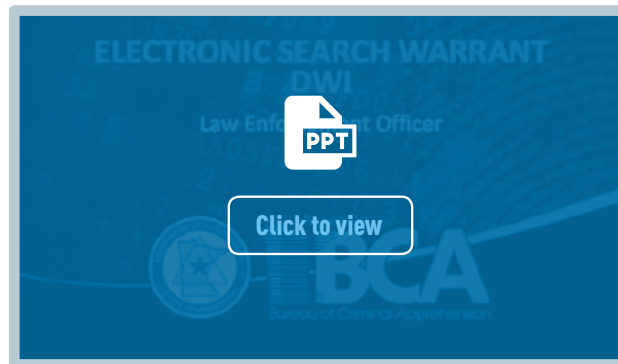
Sample Training Materials

APPENDIX E:

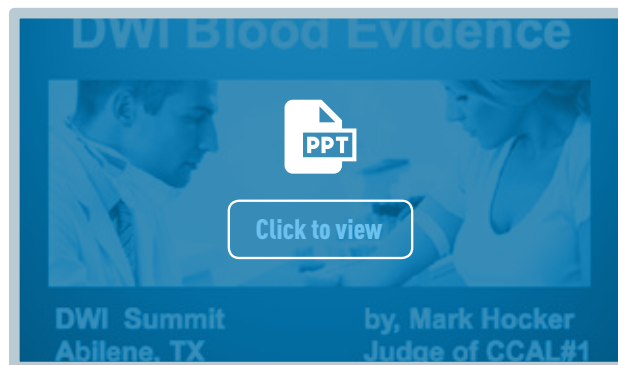
Sample Training Materials

As discussed in [Section 5](#) of this report, training of practitioners is an important component of eWarrant system implementation. This appendix contains examples of eWarrant presentations from Minnesota, Texas, and Utah that are used to deliver online and/or in-person training to law enforcement and judges. Click on the images below to access these training materials.

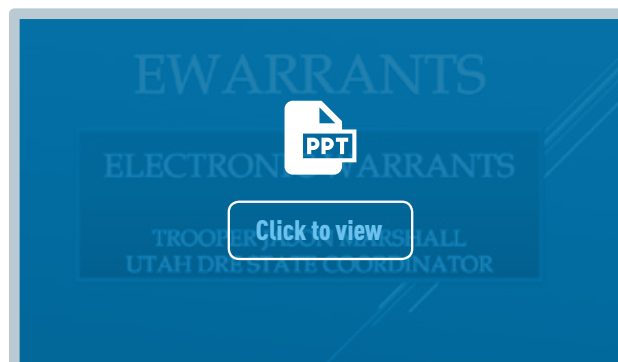
Minnesota Electronic Search Warrant Training Materials



Lubbock, Texas PowerPoint for Judicial Training



Utah DRE Training Materials



IMPROVING DUI SYSTEM EFFICIENCY

**A Guide to Implementing
Electronic Warrants**

APPENDIX F

**eWarrant System
Resources and
Visuals**

APPENDIX F:

eWarrant System Resources and Visuals

The case studies in [Section 7](#) of this report highlighted practices in five jurisdictions and included screen shots from their eWarrant systems. The following are additional screen shots from Minnesota, Utah, and Texas' systems. Also included in this appendix is a copy of the Administrative Order that authorized Maricopa County's electronic search warrant pilot in 2012.

Minnesota eSearch Warrant Screen Shots

My Work Manage Forms Notifications Preferences Reports Help

Search Warrant - Application Search Warrant Details Save successful

Search Warrant Type
Search Warrant Application
Advanced Search

Draft (you're looking at)

Document Type: Out Search Warrant Case Number: 2012010
 Submitter: AL EDWARD TWO Law Enforcement: Hennepin
 Charging Act: 609.02 Prosecution: Court
 Document Id: 22

Print Process Print

Description	Grounds	Facts	Additional Resources								
<p>Warrant to Search</p> <p>Select all applicable:</p> <p><input type="checkbox"/> Premises</p> <p><input type="checkbox"/> Motor Vehicle</p> <p><input checked="" type="checkbox"/> Person</p> <p>First Name: AL Middle Name: EDWARD Last Name: TWO Suffix: Date of Birth: 01/01/1974</p> <p>Property and Things to be searched and seized</p> <p>List all the evidence that needs to be searched and seized</p> <table border="1"> <thead> <tr> <th>Format</th> <th>Quantity</th> <th>Unit</th> <th>Notes</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td>Blood sample from AL EDWARD TWO, Date of Birth 01/01/1974</td> </tr> </tbody> </table> <p>Description of premises, motor vehicle or person to be searched, where the above evidence will be found</p> <p>List and describe in detail the premises, motor vehicle or person - where the above evidence will be found</p> <p>AL EDWARD TWO, Date of Birth 01/01/1974</p> <p>Location of Search</p> <p>City or Township of: County of: Hennepin State of Minnesota</p> <p>Save and Continue Search</p>				Format	Quantity	Unit	Notes				Blood sample from AL EDWARD TWO, Date of Birth 01/01/1974
Format	Quantity	Unit	Notes								
			Blood sample from AL EDWARD TWO, Date of Birth 01/01/1974								

Currently Assigned to: Dev Officer, at the Carver County Sheriff

Sign and Submit to Judge

I declare under penalty of perjury that everything stated in this document is true and correct.

Place of Signature

County: State:

Officer's Call back phone: (This phone number will only be visible to the assigned Judge.)

Select Judge

Courthouse: Judge:

Sign and Submit

Save and Close Save

- 2, Judge
- 3, Judge
- Carverjudge, Karen
- Dredd, Judge
- Jones, Judy
- Judge, Biometric
- Judge, DA
- judge, djc
- Judge, GT
- Judge, KR
- Judge, KS
- Judge, TM
- Judge, Tom
- judge, winona
- judge1, carver
- judge2, carver
- Schoen, Paul
- Vel1, JRams
- Vel2, JRams
- Vel3, JRams

1 / 4 Find

Application Page 1 - 2

STATE OF MINNESOTA, COUNTY OF CARVER DISTRICT COURT

APPLICATION FOR SEARCH WARRANT

The screenshot displays the eCharging application interface. At the top left is the eCharging logo. To its right is a dropdown menu for 'Current Agency/Client' and a search bar for 'First/Last name or Case/Citation #'. A 'Welcome' message and a 'Logout' link are in the top right. A navigation bar contains tabs for 'My Work', 'Manage Forms', 'Notifications', 'Preferences', 'Reports', and 'Help'. The main content area is titled 'Work Summary' and features a sidebar with 'Work - Me' and 'Work - My Agency'. The main text reads 'This is a summary of work for' followed by a blurred name. Below this are links for 'Create new eCharging form', 'Assign multiple eCharging forms', and a checked checkbox for 'Show Documents Assigned To Me For All My Agencies'. Two tables are present: 'Forms Awaiting Action' and 'Drafts'. Both tables have headers: Case Number, Type, Charge Level, Subject, Subject Status, Creation Date, Status, Assigned To, and Action. The 'Drafts' table includes the text 'No drafts available for viewing'. The footer contains '© 2013 RDA' with links for 'Privacy Statement' and 'Help', and 'Version 3.0' on the right.

Utah Criminal Justice Information System eWarrant Module Screen Shots

UCJIS Utah Criminal Justice Information System

TRANSACTION C New Broadcast Message Alan Duane Leidig (Log Out)

Close All (18) UTAH AMBER ALERT... 56:38 until timeout

UCJIS Home

+ Favorites

- ⊞ Gun
- ⊞ Article
- ⊞ Messaging
- ⊞ Vehicle
- ⊞ Other
- ⊞ LOCAL
 - ⊞ Change Password
 - ⊞ Forensic Services
 - ⊞ eWarrants
 - WE - Warrant Entry
 - EWE - E-Warrant Entry
 - EWEJ - E-Warrant Juvenile Entry
 - WEJ - Warrant Juvenile Entry
 - WJQ - eWarrant Jurisdiction Query
 - EWQ - E-Warrant Query
 - WQS - eWarrants Query Supervisory
 - EWQJ - E-Warrant Juvenile Query
 - EWQS - E-Warrant Supervisor Query
 - EWQP - E-Warrant Prosecutor Query
- ⊞ NLETS
- ⊞ NCIC
- ⊞ Person
- ⊞ Configuration

Last logged in: 03-17-2016 09:11
 Version: 1.0-SNAPSHOT.3388
 Server Node: pslweblogic-testrf2.ps.utah.gov

Note: Drag a favorite to reorder it. Right click an item to remove or add to favorites.

UCJIS Utah Criminal Justice Information System

TRANSACTION C New Broadcast Message Alan Duane Leidig (Log Out)

Close All (18) UTAH AMBER ALERT... 52:21 until timeout

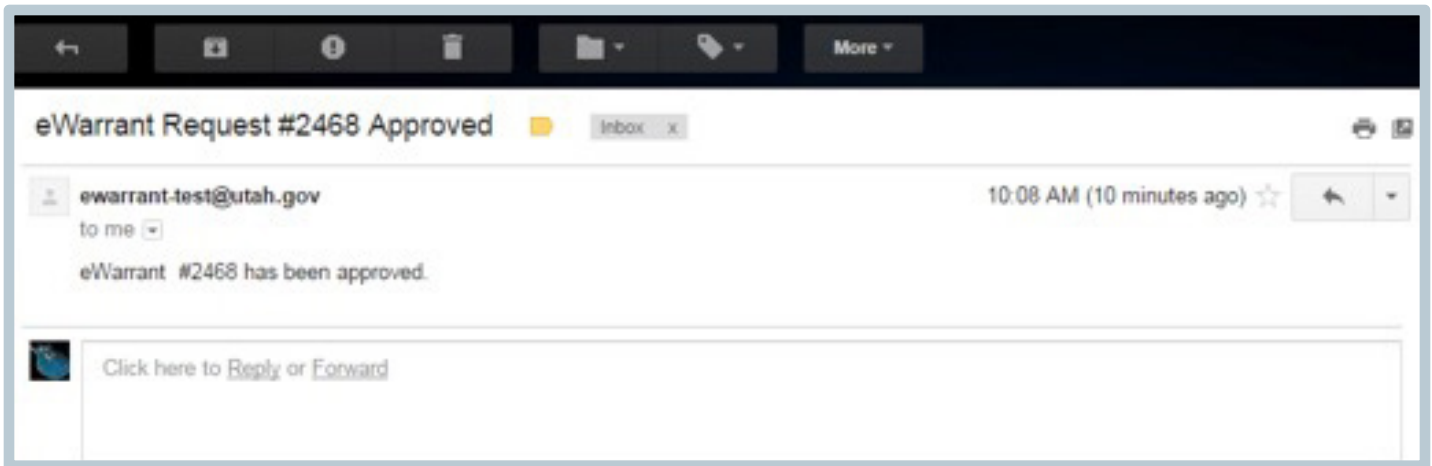
UCJIS Home

+ Favorites

- EWEL - E-Warrant Entry
- EWQL - E-Warrant Query
- ⊞ Gun
- ⊞ Article
- ⊞ Messaging
- ⊞ Vehicle
- ⊞ Other
- ⊞ Person
- ⊞ Configuration

Last logged in: 03-17-2016 09:11
 Version: 1.0-SNAPSHOT.3388
 Server Node: pslweblogic-testrf2.ps.utah.gov

Note: Drag a favorite to reorder it. Right click an item to remove or add to favorites.



eWarrant Details

eWarrant Details
Created by aleidigt on 04/05/2016 10:11:37

<p>Warrant Number: 2468</p> <p>Status: APPROVED</p> <p>Status Comment:</p> <p>User ID: aleidigt</p> <p>User Name: Alan Duane Leidig</p> <p>User Contact: 8019654739</p> <p>Jurisdiction: THIRD DISTRICT COURT - SALT LAKE</p> <p>Judge Name: TEST JUDGE</p> <p>Exclusive: No</p> <p>Notification Date:</p> <p>Submission Ready: Yes</p>	<p>Case Number:</p> <p>Status Time: Tue Apr 05 10:08:13 GMT-0600 2016</p> <p>Extended Warrant Number:</p> <p>Agency: BOFS</p> <p>User E-mail: aleidigt@utah.gov</p> <p>On: UTBC0000</p> <p>Type: DUI Blood Draw Warrant</p> <p>Judge Contact: This is a test to see if we can tell how many characters it takes to reach 155. If each line is 96 characters, we need 59 more characters. This is the End</p> <p>Sealed Date: 04/25/2016</p> <p>Original Issue Date: 04/05/2016</p>
---	--

New Options

eWarrant Options

[Status History](#)
[Affidavit PDF](#)
[Warrant PDF](#)
[Return of Service](#)
[Refresh Display](#)

UCJIS
Utah Criminal Justice Information System

TRANSACTION C New Broadcast Message

Close All (18) UTAH AMBER ALERT... 52:32 until timeout

Alan Duane Leidig (Log Out)

UCJIS Home EWEL x

Entry

eWarrant Creation

eWarrant Type*

Jurisdiction*

County*

Case Number:

Existing Warrant Number:

eWarrant Entry Wizard

Created by aleidigt on 04/04/2016 11:42:07

< Previous Page: NA **Jurisdiction Department** Next Page: Person >

- * Department
- * Person
- * Probable Cause

Officer Title*

Officer Agency*

City/Location*

< Previous Page: NA **Jurisdiction Department** Next Page: Person >

eWarrant Entry Wizard
Created by aleidigt on 04/04/2016 11:42:07

[< Previous Page: Jurisdiction Department](#) **Person** [Next Page: Probable Cause >](#)

✔ Department

✖ **Person**

✖ Probable Cause

Save

View Summary

In the body of*

Further described as*

[< Previous Page: Jurisdiction Department](#) **Person** [Next Page: Probable Cause >](#)

eWarrant Entry Wizard
Created by aleidigt on 04/04/2016 11:42:07

[< Previous Page: Person](#) [Probable Cause](#) [View Summary >](#)

✔ Department

✔ Person

✖ Probable Cause

Save

View Summary

Substance(s) in blood*

Training/Experience*

I'm so awesome that I don't need to really write anything in this space.

Probable Cause*

[< Previous Page: Person](#) [Probable Cause](#) [View Summary >](#)

eWarrant Details		Created by aleidigt on 04/04/2016 12:11:23	
Warrant Number:	2468	Case Number:	
Status:	INITIAL	Status Time:	Mon Apr 04 11:42:07 GMT-600 2016
Status Comment:			
User ID:	aleidigt	Agency:	BCIFS
User Name:	Alan Duane Leidig	User E-mail:	aleidigt@utah.gov
User Contact:		Ori:	UTBCI0000
Jurisdiction:	THIRD DISTRICT COURT - SALT LAKE	Type:	DUI Blood Draw Warrant
Judge Name:		Judge Contact:	
Exclusive:		Sealed Date:	
Notification Date:		Original Issue Date:	
Submission Ready:	Yes		

Edit Answers
Email Prosecutor
Prepare to Submit
Status History
Affidavit PDF
Delete Affidavit
Refresh Display

Affidavit PDF

Hero Statement

Your Information

Probable Cause Statement

Legal Digital Signature will appear here when submitted to the judge

The facts to establish the grounds for issuance of a Search Warrant are:

Your affiant, Alan Duane Leidig, a police officer with Gotham City Police Department, being duly sworn, deposes and states that:

I'm so awesome that I don't need to really write anything in this space.

Suspect was observed driving while drinking out of a vodka bottle.

A warrant for a blood draw is necessary to prevent the loss of evidence, to wit: through dissipation of the alcohol or any other controlled substance, from the blood.

WHEREFORE, your affiant prays that a Search Warrant be issued for the seizure of said blood at any time day or night, using a reasonable amount of force to obtain the sample.

I declare under criminal penalty of the State of Utah that the foregoing is true and correct.

Executed on: 4th day of April, 2016 @ 12:43 PM by /s/

Submit to Judge

User ID:	albridge	Agency:	BOFS
User Name:	Alan Duane Leidy	User E-mail:	albridge@utah.gov
User Contact:		On:	UTB00000
Jurisdiction:	THIRD DISTRICT COURT - SALT LAKE	Type:	DUI Blood Draw Warrant
Judge Name:		Judge Contact:	
Exclusive:		Sealed Date:	
Notification Date:		Original Issue Date:	
Submission Ready:	Yes		

[Edit Answers](#) [Email Prosecutor](#) [Prepare to Submit](#) [Status History](#) [Affidavit PDF](#) [Delete Affidavit](#) [Refresh Display](#)

eWarrant Affidavit Submission

Judge *

Your Phone #:

Request to extend Seal Date:

Exclusive to Judge:

Delay Submission:

ATTENTION: Courts systems are down daily between 0445 and 0515. Submissions during this time frame may not notify the on-call magistrate.

By submitting this affidavit, I declare under criminal penalty of the State of Utah that the foregoing is true and correct.

On Call Judge is the default in the drop down list

Texas Mynorefusal.com Screen Shots

The screenshot shows a web browser window with the URL mynorefusal.com/Forms/MSWP/MSWP4Affidavit. The page title is "New Search Warrant Affidavit". The navigation menu includes "Home", "Applications", "About", and "Feedback". The main content area has tabs for "Offense", "Evidence", "BFTs", "Other Factors", and "Affiant", with "Other Factors" currently selected. The "OTHER FACTORS AND OBSERVATIONS" section contains the following fields:

- Other Tests Performed:
- Additional Observations / Factors:
- Suspect's Oral Statements:
- Chemical Tests Offered (but Refused):
- Portable Breath Test Result:

At the bottom right of the form, there are "Next" and "Prev" buttons. A copyright notice "© 2017 - No Refusal" is visible in the bottom right corner of the page.

Maricopa County Electronic Search Warrant Pilot Program Administrative Order

IN THE SUPERIOR COURT OF THE STATE OF ARIZONA
IN AND FOR THE COUNTY OF MARICOPA

IN THE MATTER OF ELECTRONIC) ADMINISTRATIVE ORDER
SEARCH WARRANT PILOT PROGRAM) NO. 2012-111
_____)

WHEREAS, Arizona Supreme Court Administrative Order 2012-15 authorizes an electronic search warrant pilot program in Maricopa County; and

WHEREAS, the Superior Court in Maricopa County has developed a reliable and secure system for exchanging electronic documents and signatures between the court and law enforcement agencies for the purposes of this pilot program,

IT IS ORDERED that the attached policies and procedures for the electronic search warrant pilot program be adopted.

IT IS FURTHER ORDERED that this order shall terminate at the end of the two-year pilot program unless otherwise ordered.

Dated this 20th day of July, 2012.

[Click to view](#)

Norman J. Davis
Presiding Judge

- Original: Clerk of the Superior Court
- Copies: Hon. Douglas Rayes, Criminal Presiding Judge
All Criminal Judges and Commissioners
Hon. Tom Horne, Attorney General
Hon. Bill Montgomery, County Attorney
James Logan, Public Defense Services
Jim Haas, Public Defender
Marty Lieberman, Legal Defender
Bruce F. Peterson, Legal Advocate
Phil Knox, General Jurisdiction Court Administrator
Bob James, Criminal Court Administrator
Det. Dan Mulleneaux, Phoenix Police Department
Sgt. Douglas Opferbeck, Phoenix Police Department



FOUNDATION FOR
ADVANCING ALCOHOL
RESPONSIBILITY



responsibility.org/blog



twitter.com/goFAAR



facebook.com/goFAAR



youtube.com/goFAAR



instagram.com/go_FAAR



flickr.com/goFAAR



pinterest.com/goFAAR



responsibility.org/get-the-facts



BACARDI U.S.A., INC.

Beam SUNTORY



BROWN-FORMAN



Constellation Brands

DIAGEO



EDRINGTON



Jägermeister
MAST-JÄGERMEISTER US



Pernod Ricard USA

2345 Crystal Drive
Suite 710
Arlington, VA 22202
202-637-0077

[RESPONSIBILITY.ORG](https://responsibility.org)