Protection Order Repositories, Web Portals, and Beyond

TECHNOLOGY SOLUTIONS TO INCREASE ACCESS AND ENFORCEMENT

This project is supported by Grant No. 2016 TA-AX-K054 awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice, Office on Violence Against Women.

CONTENTS

Center for Court Innovation

BATTERED WOMEN'S JUSTICE PROJECT
National Center on Protection Orders and Full Faith & Credit

NCSC
National Center for State Courts

CHAPTER 1

Introduction

1. Introduction

956,586

The civil protection order caseloads reported by 49 states, the District of Columbia, Guam, and Puerto Rico in 2018.

Since the early 1990's, protection orders have been a potentially powerful tool for enhancing safety, economic security, and well-being for survivors of domestic violence, sexual assault, stalking, and dating violence.[1] The potential benefits of protection orders have always been constrained by an array of factors, beginning with limitations on safe and informed access to courts to obtain an order and continuing with impediments to the enforcement of orders. Perhaps chief among these impediments are physical and technological obstacles to transmitting protection order data across local, state, and federal systems, which can thwart timely service of orders on defendants, cause delays in court proceedings, render records systems unreliable, and prevent verification of valid orders needed for enforcement by law enforcement, prosecutors and judges.

One of the key strategies for ensuring enforcement of protection orders has been the development of federal and state repositories of electronic protection order records. In 1997, the Federal Bureau of Investigation established the National Crime Information Center Protection Order File (NCIC POF) to serve as a national repository for protection orders.[2] (See Section III for discussion of the NCIC POF.) Participation in the NCIC POF is not mandatory, and so its potential to serve as a reliable and comprehensive national repository has not been fully realized. Most states have created centralized repositories of protection orders issued in their state to allow verification of valid orders and to transmit protection order data to the NCIC POF. States vary greatly, however, in their capacities to conform their data and verification procedures to the requirements established by the NCIC POF. Consequently, a significant number of state and tribal protection orders are not entered into the NCIC POF.[3]

Over the past several years, courts, justice system partners, and domestic violence advocates have collaborated on improving their protection order repositories and transmission of data to the NCIC POF, as well as developing more advanced technology solutions to reduce barriers to protection order access and effective enforcement. These technologies include web portals and e-filing that are aimed at improving the ease, safety, and speed of protection order filing, and emerging technologies that can enhance the efficiency and security of protection order data exchanges.

This report provides an overview of state protection order repositories and issues that impact transmission of data to the NCIC POF; offers guidance on the basic elements of designing, developing, and improving the quality and security of protection order data exchanges; and highlights state efforts to apply innovative technologies to their protection order systems. The report is designed for policymakers and practitioners within courts, advocacy organizations, IT departments, and law enforcement agencies who are considering ways to increase online access to protection orders, reduce opportunities for errors and delays that can result from reliance on paper and manual processes, and achieve more effective enforcement through faster and more reliable data exchanges.

CHAPTER 2

Design and Development of Protection Order Data Exchanges

2. Design and Development of Protection Order Data Exchanges

The design and development of protection order data exchanges require consideration of several factors specific to the purposes of protection orders. The information collected for a protection order petition is sensitive, has personally identifiable information (PII), and must move rapidly. Although in some instances paper files are necessary, they are inherently inefficient because they often contain incomplete information, have illegible handwriting, and require that the information provided be keyed into a case management system.

Electronic systems can address these deficiencies through quality control checks such as preventing a filer from moving forward in a petition unless a required element is provided, providing a pick list of choices, and a host of other means to assemble an electronic document that is complete so that the court may consider the petition and move forward. Incomplete information in both electronic and paper forms causes delays, so quality control measures are important to inlcdue in the design of electronic formats.

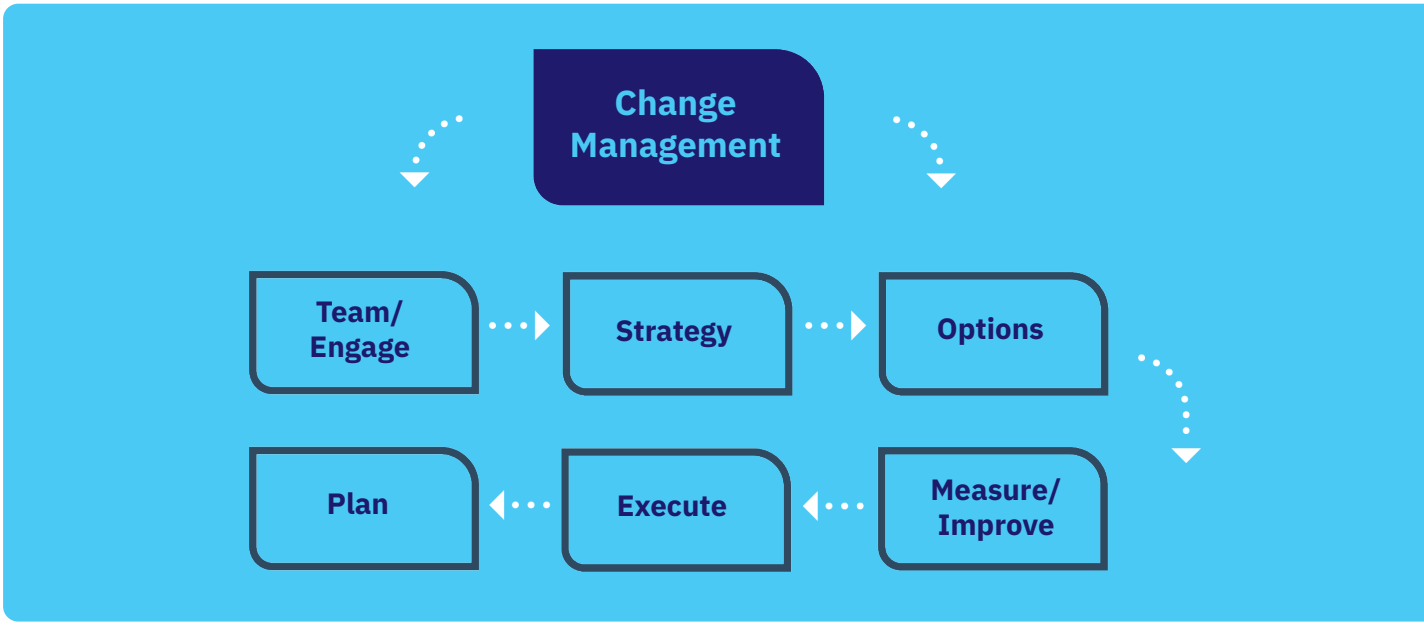
Another advantage of electronic data is that it may be transmitted through various means. Using data exchanges between the various stakeholders covers each touchpoint seamlessly. This starts with the creation and submission of the documents, receipt and docketing by the clerk/court, process service, the court filing a decision order (granted/denied), and law enforcement that must serve the granted orders and report them to NCIC. Additionally, data exchanges also allow for quality control measures after transmission such as verification of successful/unsuccessful transmission as well as identification of errors that must be corrected.

2.1. Change Management

Change management is central to the governance of initiatives to create data exchanges between multiple participating stakeholders. As the need to share data increases, there can also be an increase in competing demands for changes to application systems and data content. As part of a governance structure, a formal change management approach is needed to control application costs, have stakeholder agreement on changes, their implications, and timing of change implementation, and a continued focus on data quality, data access methods, and continued development and adherence to policy and other legal requirements. To have successful change management, it is important to understand the various roles within each organization to have the correct subject matter experts involved.

- **Business Analysts –** This group is the primary group to lead the change management process and are the primary subject matter experts of the needs of the application users and data consumers. They look at existing processes and determine areas for change and improvement and then verify that these have been accomplished after changes have been incorporated.

- **Information Technology –** Information technology focuses on the development of the platform(s) that house applications and data, monitoring of hardware/storage capacity and communications, patch management, and network security. They also work with application developers on performance monitoring as it relates to hardware, cloud, communications, and other infrastructure.
- **Vendors –** for vendor owned applications, having the authoritative group for changes and a primary product owner identified is important.



2.2. Data Quality

Data quality measures and processes should be planned as part of the development of the exchange. For protection orders, data quality often begins at the intake process. Intelligent application design will use methods such as drop-down pick lists that limit the selection of choices to a consistent standard. Rules that prevent moving forward unless key information is provided will confirm that needed information is collected at the appropriate time. Automated processes may be used to link related records, identify duplicate records, and check for other data issues. These processes will help with data quality and reduce potential delays caused by missing or inconsistent information. Quality measures may include analysis of incorrect selections or other areas that cause delays due to incorrect or incomplete information. This may lead to improvements in the process by having a better understanding of how the user is interacting with the data collection process.

Records updates and changes are controlled by user access levels that control who can view, create, update, or delete information. Role-based access is a common approach to managing records' updates. In Iowa, for example, only the clerks can change incorrect information on orders. They then notify the Department

of Protective Services by resending the order. Clear rules on user access and automated data validation can improve data quality. Having multiple repositories can result in lower quality data.

For example, New York has two repositories: 1) the New York State Unified Court System's statewide case management system, which is the originator of the record and sends the data to NCIC, and 2) a New York State Police portal (NYSPIN) that transfers to NCIC. This split model may result in conflicting records in NCIC and in the two systems. To address this problem, the statewide court case management system and the state police must periodically reconcile their records, which is time-consuming task. In turn, the state police do the same with NCIC. Most states, however, have one audit per year conducted by an outside auditor.

2.3. Security

Each state has a legal framework governing the access and control of information within cases or case types that are deemed sensitive and confidential. A framework can be developed that defines user roles and levels of access and permissions by role. User roles may be adjusted as legislation and other factors influence access rights.

Some states have a simple framework with two levels of access. For example, in Iowa, the levels of access include 1) less than full for those in the field who are just entering data; and 2) full access (e.g., Court Clerks, Department of Public Safety). Those with full access must go through training and re-certify every two years to enter and reviewdata. In Alaska, the two levels of access are for data entry or queries.

The user roles framework, in conjunction with an established privacy policy, can also be used to ensure only the appropriate users can access certain records, thus preserving the privacy of records. Security of data systems goes beyond access controls, however. Transfer methods are secured by using encryption and access controls that identify authorized transfer points and restrict data acceptance to only those registered transfer points. Florida's detailed access security matrix by user role can be accessed here.

Monitoring software is recommended to watch access times, frequency, and user account access at the record level; changes to user accounts (including creation and deletion); date and time of record creation; data transfer failure or success; and general network health and availability. Monitoring often includes automated alerts for activities outside of normal thresholds such as frequent access by a user account outside of normal business hours. The more advanced systems can also retrace the activity of users. Monitoring also is helpful for the technology department to be alerted to and address suspicious or malicious activities.

Application logs are inherently included in most software. Logging various events can alert for suspicious activity, be used to investigate questions about records changes or deletions, and be viewed for general audits looking at activity. Common logged events may include data and time of record creationl; user account access at the record level; creation; change and deletion of user accounts; and automated data exchange processes.

CHAPTER 3

Protection Order Repositories

3. Protection Order Repositories

A general definition of a repository is "a place where things are stored or can be found."[4] In computing, the term is generally used to refer to "a central location in which data is stored and managed."[5] A protection order repository refers to a centralized location where protection order-related electronic data can be filed, maintained, and searched.[6] Additional names for repositories used by the various states, territories, and tribes include registry, database, electronic file, and system.

48
States and territories with statewide protection order repositories.

3.1. State Protection Order Repositories

Most states and territories have statutory provisions for the recording of protection orders,[7] but there are as many variations in those provisions as there are states. Forty-eight of the 56 states and territories (hereinafter collectively called states) have statewide protection order repositories. Some of these are stand-alone, meaning that the repository does not exist within a larger statewide system, such as a criminal history repository, while others are simply records or files within another statewide system. Eight states do not have a state-specific protection order repository; instead, they rely on the National Crime Information Center's (NCIC) Protection Order File (POF) to act as the centralized repository for their information.[8]

3.1.1. Authority for state protection order repositories[9]

- **Thirty-two jurisdictions** have a protection order database or registry established by statute or require the entry of orders into an established database or registry system.
- **Other states** that do not have repository statutes have information embedded in their protection order statutes.
- **Twelve jurisdictions** specify in significant detail the procedures by which their databases are managed.

3.1.2. Types of orders and documents in state repositories

The type of orders that are allowed entry into the state repository is often set by statute.[10] All state protection order repositories contain final domestic violence protection orders, while some states allow or require the entry of other types of orders to facilitate their enforcement. For example, the entry of ex parte orders helps increase the effectiveness and timeliness of service by identifying individuals not yet served, making the orders available online, and allowing an officer to serve the order on the respondent during other interactions, such as a traffic stop. Other types of orders may be entered because they include protection order provisions as part of the order. Examples include child custody orders, consent agreements, divorce decrees, criminal pretrial release orders, and sentencing orders.

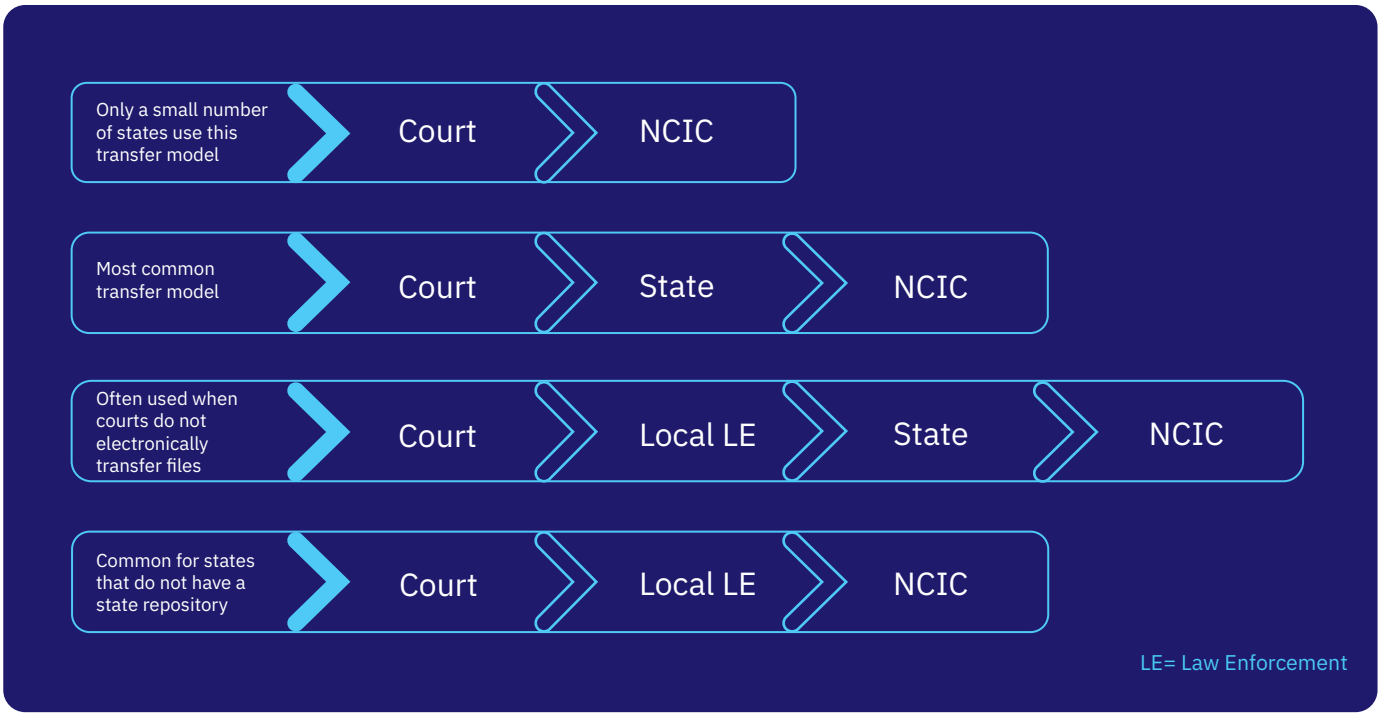
Examples of other types of orders contained in state repositories include:

- emergency, ex parte, and/or temporary orders
- stay-away or no contact orders
- stalking protection orders
- sexual assault protection orders
- orders against harassment
- juvenile protection orders
- criminal protection orders
- orders protecting elders or dependent adults
- military protection orders
- extreme risk protection orders

In addition to the protection order itself, repositories may include documents or additional information related to the order. The most common additional document is the notice of service. Including notice of service within the repository verifies that the order is in effect, eliminating the need for officers to spend time checking on notice if they are called to a scene for a violation of the order. Some states include non-protection order-related information in their repositories. For example, New Jersey's statute includes information about people who have been charged with or convicted of domestic violence crimes or violations of domestic violence-related court orders.[11]

3.1.3. Models of protection order data transfer

The following graphic is a simplified representation of the transfer points for a protection order after a court has issued it. The goal is to achieve entry of all valid orders into the NCIC POF as quickly as possible. The technologies supporting the exchanges of protection order data vary across the states and within these transfer models.



The transfer path and methods can impact the time it takes for orders to be entered into state repositories and the NCIC POF. The 2016 Survey of State Criminal History Information Systems noted the elapsed time from issuance to entry in the state protection order repository was one day or less for 22 states and two-to-seven days for 11 states. Nineteen states reported being able to enter protection orders into the NCIC POF within one day or less, while in 14 states the process might take up to seven days.[12] Some states have statutorily mandated the amount of time allowed for the entry of protection orders. For example, Mississippi specifies that orders must be entered "within twenty-four (24) hours of issuance with no exceptions for weekends or holidays."[13]

3.1.4. Models of storage and transfer

Many state repositories have used traditional methods to gather and store protection order information. Traditional methods include having server hardware on-premises to the organization and storing the data within internally controlled systems. Now that cloud-based technology is solidly established in the government domain, there has been a slow paradigm shift to cloud computing services where storage and access are contracted to a service provider that allows for services and storage to be scalable and have greater resiliency against outages. Regardless of which storage technology is used, local agencies can transfer data to the repository through a variety of methods. Transfer methods may include electronic push of information to a File Transfer Protocol (FTP) server or Secure FTP server using encryption where it will be picked up and added to the repository. Another method is the use of direct electronic connection using XML or an Application Programming Interface (API) where the data is pushed to the repository electronically. Usually, the transfers are done at a specific designated time each evening, but as technology continues to improve, more frequent daily updates close to real-time may be achieved. Each state implements the systems of storage and transfers within the context of their state's legal requirements, and therefore each may vary in the collection method and data content placed into their repository. However, each state generally has a central repository or authorized application that stores collected information from one or more sources. This central repository then connects to NCIC for data transfer or the repository connects to an authorized agency such as the state police to push the information to NCIC. This transfer must comply with NCIC standards for security and data transfer (see the section on NCIC below). The data transfer to and from the central repository can be real-time or schedule based.

3.2. Measuring the Quality of Data Exchanges to Improve State Repositories

There are several standard ways to measure the success or failure of any data-intensive project. In his book, "Designing Data-Intensive Applications,"[14] Martin Kleppman details the aspects that all such projects should consider. These include reliability, scalability, and maintainability.

3.2.1. Reliability

Reliability speaks to the ability of the application to provide:

- Performance of the function that the user expects.
- Tolerance of user mistakes or varied uses of the software.
- Adequate performance for the use case it was intended for, under expected load and volume.
- Prevention of unauthorized use and access.

Reliability may be impacted by hardware, software, and/or human faults. While hardware faults may be addressed by redundancy, software and human faults

are less easy to predict and plan for. Additionally, in cloud environments, hardware and network faults are often less easy to control in that the environment may not be directly under the control of the business using them. This often results in the design needing to be more distributed in nature.

3.2.2. Scalability

Scalability involves consideration of whether an environment will tolerate increased load and have adequate performance over time. It includes consideration of latency and response time. For protective order exchanges, the desire to have "near real-time data" causes concern about the scalability of any solution that is under consideration. Delays in time may affect the safety of protected persons.

3.2.3. Maintainability

Most of the costs of software evolve from maintenance rather than initial purchase and implementation. There are three primary considerations for maintainability: operability, simplicity, and evolvability.

- **Operability** involves the ability to perform routine tasks easily by providing visibility into the internal operations of a system through an easy operational model and documentation and predictable behavior.
- **Simplicity** means managing the complexity of a project such that it is not made more difficult and costly than it needs to be. Simplicity may involve providing technical staff with interfaces and tools that they are accustomed to using or providing interfaces that abstract the underlying complexity of the software.
- **Evolvability** provides for expansion of the solution when unexpected functionality is discovered or business priorities change. Simple and easy to understand systems are generally better understood and thus easier to evolve.

Considerations for creating or improving a protection order repository:

- Develop access and confidentiality protocols for the database.
- Define time requirements for entering orders into the state and federal repository.
- Include data that will increase the likelihood of service, enforcement, and officer safety.
    - Immediately enter ex parte orders as soon as issued into the state and federal databases (service can be updated in the MISC Field in NCIC POF).
    - Use of short-form notification may be helpful in this process.
    - Use standardized forms that include sufficient numeric information to allow for entry of the order into NCIC POF.
    - Date of birth is the preferred numeric identifier in NCIC and the information most likely available to the petitioner.
- Develop forms and protocols that facilitate entry of foreign protection orders in the registry.
- Devise training protocols for all system actors on the purpose, use, and policies of the state and federal database.
- Ensure agency policies allow for the timely update of any protocols, or procedures as needed.
- Create a sustainability plan for funding technology changes for the database.

3.3. National Crime Information Center (NCIC) Protection Order File (POF)

The FBI established the NCIC POF in 1997 to serve as the national registry of protection orders.[15] Participation in the POF is voluntary, but nine states and one territory statutorily require the entry of protection orders into the NCIC POF,[16] and most states transmit orders to the POF.[17] Protection orders in the NCIC POF must be validated regularly to ensure that they are still complete, accurate, and active.[18]

Because the NCIC POF does not contain all protection orders issued by state and tribal courts, it is an imperfect tool. Nevertheless, making protection orders available through it is an important way to help facilitate their enforcement. For example, a valid protection order is enforceable even if not entered into the NCIC POF, but entry into NCIC POF can assist enforcement when a protected party asserts that a valid protection order exists but does not have a copy or where the respondent falsely asserts he or she has not received notice of the order. The NCIC POF also facilitates the implementation of the Full Faith and Credit provisions of the Violence Against Women Act (18 U.S.C. § 2265).

Another reason for entering valid protection orders into the NCIC POF is to ensure that they are available for a National Instant Criminal Background Check System (NICS) search. NCIC POF is one of the files included in a NICS background check and is thus searched prior to a firearm or explosives being transferred to a potential buyer. If the NICS check reveals that the person is subject to an active protection order, additional research can be conducted to determine if the conditions of the order meet the requirements of 18 U.S.C. § 922(g)(8) and prohibit the transfer.

The NCIC POF has extensive rules and requirements for entry of orders into it, which creates technology and process challenges for states and tribes seeking to transmit protection orders to it. These challenges include having the ability to enter all the required elements, to provide 24/7 hit confirmation, and to have access to certain documents to "pack the record".

3.3.1. NCIC required data elements

In addition to administrative information about the agency transmitting the record, the data elements listed below are required for a protection order [19] to be entered into the NCIC POF. [20] If any of these data elements are missing from the record, the protection order cannot be entered.

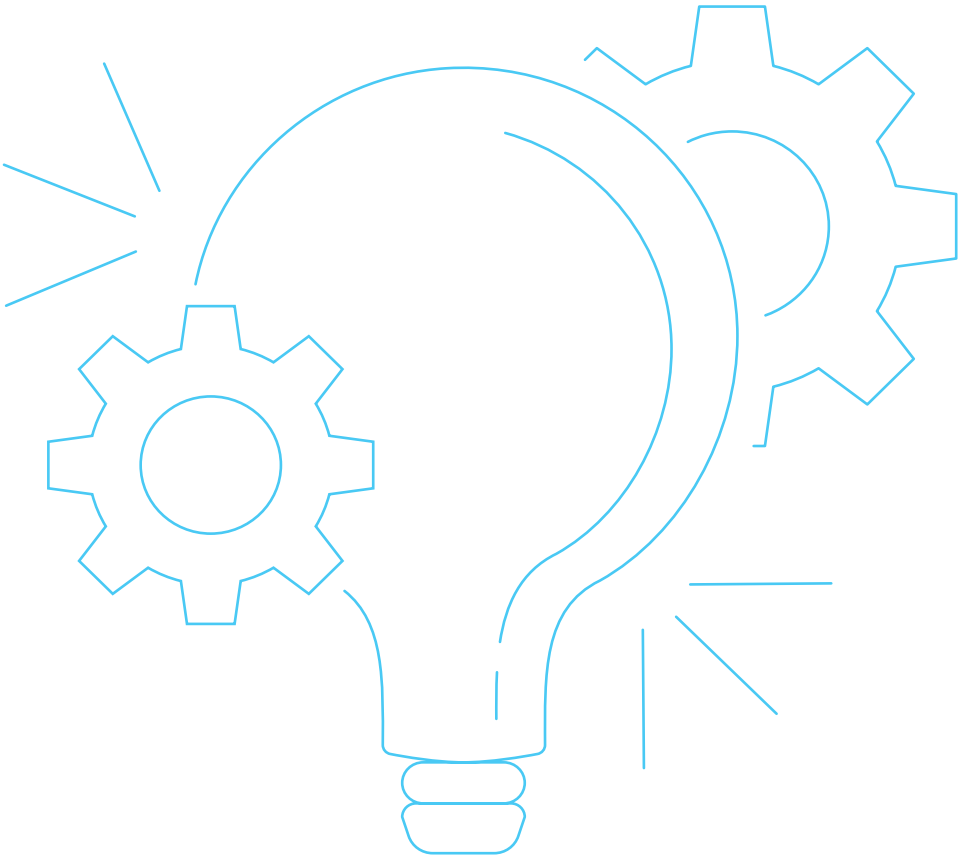
- Type of protection order (emergency, temporary, final, etc.)
- Name, sex, and race of the person against whom the order was issued
- Protection order conditions
- Date of issue
- Date of expiration
- Originating case number/protection order number
- At least one of the following: offender's date of birth, FBI number, social security number, operator (driver's) license number, vehicle identification number, or miscellaneous number (other government-issued identification documents such as a state identification or passport).

3.3.2. 24/7 hit confirmation requirement

The NCIC POF requires that the validity of all protection orders be confirmed—i.e., the order is complete, accurate, and active. This means that when a querying agency obtains a hit on a protection order record, the entering agency must be able to confirm the status and terms of the order to the querying agency before the agency can take action based on the NCIC record, such as arresting or charging a person for violating the protection order. [21] The entering agency must either have the ability to provide this service 24 hours a day, 7 days a week, or must obtain the written agreement of another agency that it will provide responses to hit confirmation requests. [22] New York is an example of a state where the state police can confirm hits because it maintains NYSPIN (New York State Police Information Network), which is the official protection order repository.

This requirement creates a problem in states where the court is the custodian of the record – i.e., the administrative office of the courts (AOC) or supreme court manages the state protection order repository, or local courts send records directly to NCIC. Courts or AOCs may not be fully staffed 24 hours a day, 7 days a week to allow person-to-person communication to confirm the validity of an order.

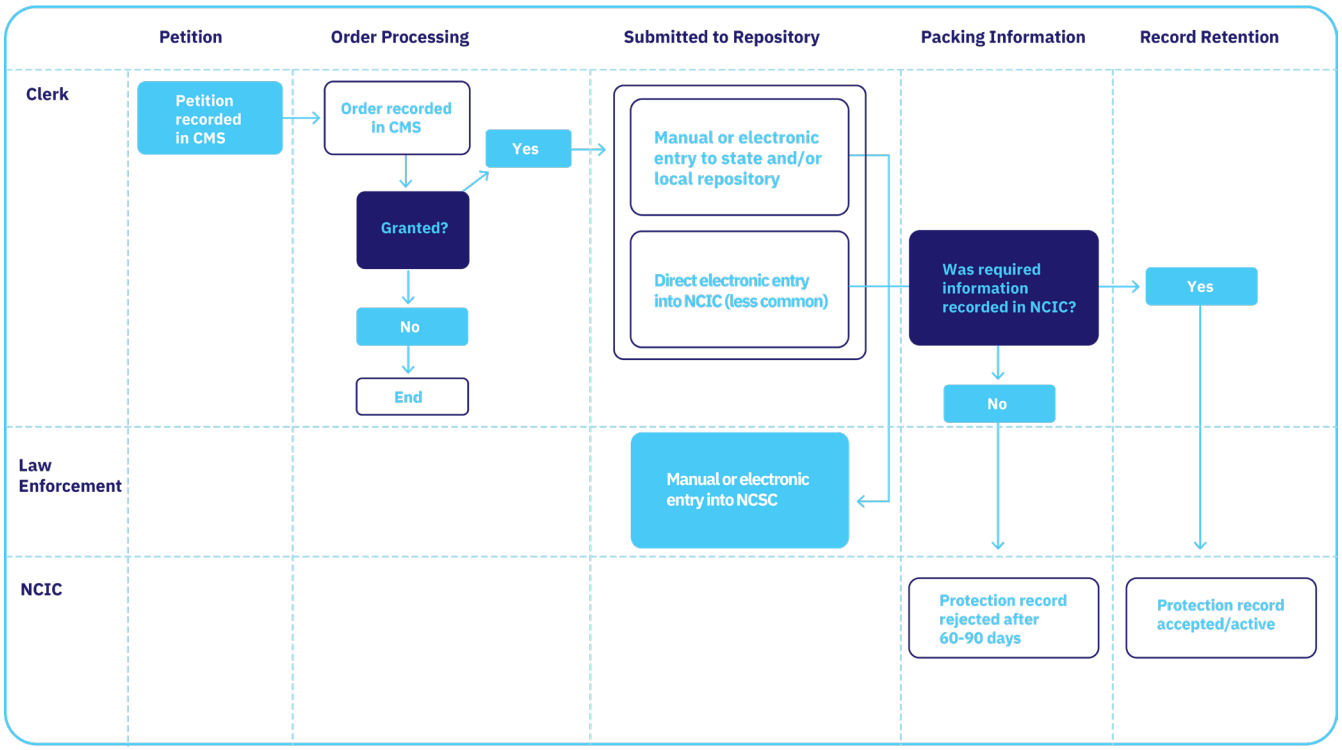
One solution to this problem has been NCIC's acceptance of scanned documents and electronic databases as the source document for the protection order, essentially allowing for hit confirmations to be obtained by electronically confirming that the protection order is still active in the state's protection order repository.[23] Arizona developed its Court Protective Order Repository, maintained by the Supreme Court of Arizona, to automate the protective order system and allow more efficient transmission of protection order data to NCIC, as well as to provide electronic hit confirmations.



3.3.3. Importance of packing the record

Packing the record means that the person entering the protection order must consult source documents (e.g., driver's license file, criminal history file, vehicle registration database) to ensure that as much descriptive information as possible about the subject of the protection order is included in the NCIC POF entry. This information is beyond the data required for entry into NCIC POF and can include physical descriptions such as eye or hair color, height, and tattoos, or potentially identifying information such as vehicle descriptions.

Consulting the source documents must be done within 60-90 days of the initial NCIC entry as well as yearly and whenever the protection order is modified. When staffing is an issue, states may not be able to enter a protection order into NCIC because they will be unable to meet this requirement. In addition, since the order is initiated by courts that do not have access to criminal history information, there may be situations whereby law enforcement is not able to or aware that the record needs to be packed. The process for packing the record is illustrated below.



CHAPTER 4

Technology Advancements to Speed Protection Order Filing and Transmission

4. Technology Advancements to Speed Protection Order Filing and Transmission

Technology provides opportunities to improve access, offers guidance and assistance through the filing process, provides better communication for phases of a protection order from filing to expiration, and improves accountability and security while allowing discrete access to various stakeholders and service providers. This section highlights Indiana's experiences in developing and implementing technologies to improve its protection order system and describes other examples of the use of web portals and e-fling in Arizona, Florida, and North Carolina. It concludes with a brief discussion of emerging technologies that can offer efficient and secure methods of protection order data exchanges.

4.1. Portals and e-Filing

4.1.1. Indiana Protection Order e-Filing, Protection Order Registry, and Advocate Access

INDIANA
sees about 35,000 new filings each year.

Like many states, Indiana has continued to respond to the changing needs and advances in technology to improve the civil protection order process, which sees about 35,000 new filings on average each year. In 2015, Indiana implemented a statewide electronic filing system (EFS) that provided for the electronic filing of new court cases and subsequent filings for most case types, but which excluded civil protection order cases due to the sensitive nature of protection order filings and the identifying information they contain. Indiana subsequently developed and implemented a separate Protection Order e-Filing Service Provider to electronically file protection orders and subsequent pleadings in protection order cases. The Protection Order EFSP includes protections and functionality specific to this case type such as form completion and document assembly.

Phased in Approach

Many applications are built and put into production in phases. This is especially true when it changes the medium (e.g., paper to electronic) and rules of procedure or there are multiple case management systems in use. Additionally, certain case types have unique requirements and challenges, so often courts will have a phased approach to implementing electronic filing and other services provided by electronic portals. Indiana's model has multiple third-party e-filing service providers and even though these service providers exist independently from the Protection Order EFSP, the filer can use the same credentials for any EFSP for ease of use.

Case Management System

Indiana selected Tyler Technologies' Odyssey as its case management system (CMS) and plans on having it statewide by the end of 2021. The Protection Order Registry interfaces with Odyssey. Indiana's Protection Order Registry and Odyssey allows judges to work remotely and use digital signatures. Currently, Protection Orders are generated in the Registry and transmitted to Odyssey, which greatly improves accuracy and timeliness.

Protection Order Registry

Indiana began implementation of a centralized protection order registry (POR) in 2007. In 2009 the legislature required the POR to operate statewide and that judges, clerks, and law enforcement use it. The POR interfaces with the Indiana State Police system called IDACS. This allows court orders and the necessary identifiers to be pushed electronically to the state police and NCIC. Local law enforcement agencies also have access to orders in the POR including information on where the petitioner and respondent reside. Using one centralized system helps ensure data accuracy. Indiana uses required standardized forms for protection orders that help ensure all required data for protection orders and entry into NCIC is provided. Orders are stored within the centralized protection order registry, and they include 1) criminal No Contact Orders, 2) Workplace Violence Restraining Orders, and 3) Child Protection Orders in addition to 4) civil protection orders.

Advocate Access

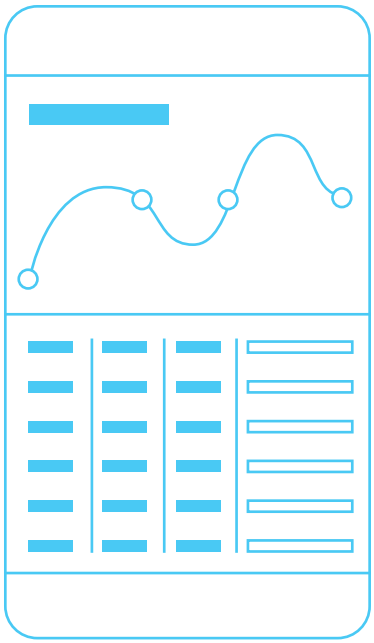
After Indiana completed the deployment to all counties of its statewide protection order registry in 2009, it also deployed a special module connected to the registry called "Advocate Access" to collect information and generate documents required to file a petition for a protection order . The forms module carries over common information such as name and address to all forms to reduce data entry. Using Advocate Access, advocates assist survivors in filing their protection order petitions from remote locations such as shelters, law offices, social service agencies, and hospital emergency rooms. Advocates first discuss safety planning and provide guidance on the potential consequences of seeking a protection order. They also provide additional support and resources. Regular training is provided to all advocates to maintain a high level of confidence in use of the system.

For survivors who decide to proceed, advocates help them complete the forms and review them to make sure they are accurate. The advocate can then either print out the forms for the survivor to file with the court in-person or submit the forms to the registry, where the case is generated and transmitted to the court's CMS. A flowchart of petitions created through Advocate Access can be accessed here. Advocates also provide a signed paper copy that includes a petition number that may be used by the clerk to find the electronic file in the registry. When advocates create a new case using Advocate Access, the data from the case is automatically entered into the protection order registry (POR), which eliminates duplicate data entry by the court clerk.

A popular feature that was added in 2011 was the ability for a survivor to sign up for text, email or fax notification. These notifications were delivered at two critical times: (1) when the Order was served on the respondent; and (2) when the Order was about to expire. Since that time, fax notifications are no longer offered but text and email notifications remain popular.

Protection Order eFiling Service Provider (EFSP)[24]

Building on the functionality of Advocate Access and the statewide electronic filing system, the Supreme Court



collaborated with advocates, law enforcement, and other justice system stakeholders to launch a separate protection order electronic filing service provider, the Protection Order EFSP. This service increases court access by allowing victims to e-file for a protection order without the risk of presenting at the courthouse. They can file from a library, home, shelter, or other secure location. Any connection to the internet will allow them to complete the petition electronically, yet they continue to have ready access to an advocate during the filing process.

A wizard guides the filer through the process and allows the user to upload optional supporting documents. The system provides the capability to save information, so the filer may return later to complete the process if there is an interruption. There are several safeguards built into the system. For example, the system provides links to advocates and service providers in each county, as well as links to hotline and chat services. On every page, filers can stop, save their work and contact one of the service providers for help. The system also provides escape buttons on every page that, when clicked, launch a new website immediately. New enhancements are being made to the Protection Order EFSP to allow the judge and the filer to communicate electronically or by other selected means if there are questions about information the filer provided. This communication will reduce delays if there are questions that must be addressed before the judge issues an order.

The information entered by the petitioner into the system is transmitted to the court's CMS through the statewide e-filing system as well as to the statewide Protection Order Registry. A flowchart of petitions filed through the EFSP can be accessed here . This technology reduces data entry and errors because the filer provides the information electronically, which allows the applications to consume it directly rather than being manually entered into each system. Indiana continues to provide training to judges, court staff, and advocates on the use and benefits of the service.

Notifications

As part of the integration and interfaces between the CMS and registry, the protected person may opt in to receive notifications. Notification methods include email, text, or both. Notification messages include but are not limited to Order Granted, Order Expiring, service attempted, and service perfected.

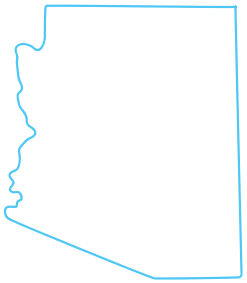
Governance

Indiana's Protection Order Committee, composed of judges, clerks, and other stakeholders, provides governance for protection order systems and processes. The Protection Order Committee oversees forms, system implementation, and changes within the protection order registry. The impetus for implementing the Protection Order EFSP was twofold: (1) Indiana wanted every case type to be included in the statewide e-filing system; and (2) the Committee wanted to ensure that federal guidelines for confidentiality of the survivor were followed and that all required data was collected at the time of filing. The Committee also considered the issues arising from the high proportion of protection order petitions prepared and filed by self-represented litigants who lacked information needed for filing the petition. Building an application that collected the needed information from filers delayed the process. The Committee guided the development of the PO EFSP to include the tools and information that would safely assist self-represented filers, whether they worked directly with an advocate or not.

4.1.2. AZPOINT, the Arizona Protective Order Initiation and Notification Tool

Arizona's Statewide Protective Order Project 2020 was deployed on January 1, 2020. The project includes two components. The first is the Court Protective Order Repository (CPOR) maintained by the Supreme Court of Arizona. CPOR is a statewide database for Orders of Protection, Injunctions Against Harassment, and Injunctions Against Workplace Harassment and transmits served orders to NCIC. The second component is AZPOINT which includes a petition portal, a clerk portal, and a service portal.[25] AZPOINT can be accessed here. The petition portal is accessible on laptops, smartphones, and other devices. Survivors can use the petition portal to complete applications for orders of protection, injunctions against harassment, or injunctions against workplace harassment. The portal uses an interview structure to assist plaintiffs in determining eligibility for requesting an order of protection and to gather the information needed to complete necessary court forms. The portal saves information for 90 days, allowing plaintiffs to return to the system as many times as needed. This gives plaintiffs the opportunity to contact an advocate during the process for assistance with the petition, information about the court process, and help in safety planning.

AZPOINT
prioritizes plaintiff safety and access to advocacy services.



Once the minimum required information is entered, the portal issues a petition confirmation number that court staff use to access plaintiff's forms through the clerk portal. When a plaintiff is ready to file, he or she goes to a courthouse and provides the confirmation number to court staff, who downloads the petition through the clerk portal and files the order in the case management system.[26] The service portal allows law enforcement to access the order of protection, print out the service packet, and file a declaration of service after the order has been served. Plaintiffs can opt in to receive notice of service.

In addition to providing access to the guided petitioning process, AZPOINT provides a wealth of information for plaintiffs, including how to find a victim advocate, how to get help with their case, and how to stay safe while seeking assistance. The Frequently Asked Questions (FAQ) page of the portal is divided into sections for general questions about orders of protection, resources for victim support, information regarding online safety, and troubleshooting the user account. There are multiple safety reminders throughout the site, along with advice on how to be proactive in remaining safe during the process of requesting an order of protection. Online safety is of particular concern so there is a safety button to log the user out of the portal, redirecting their browser to a Google search page, as well as guidance for ensuring that they are using a secure computer and instructions for how to privately browse the internet.

4.1.3. Florida eFiling and Court Services Portal

Florida has developed a portal that provides multiple services such as electronic filing of court cases, process service, and filing of court orders. The portal includes filing and service for attorneys as well as self-represented litigants including the ability to electronically file protection order petitions.

There are 5 protection order types in Florida: 1) Domestic Violence, 2) Stalking Violence, 3) Repeat Violence, 4) Sexual Violence, and 5) Dating Violence. There are standard petition forms for each type of that may be downloaded and

Florida's "eProtection Orders" initiative builds on its eWarrants platform to better track the status of orders and provide electronic notifications.

completed. Self-represented litigants may file on paper with the clerk in the county where the event occurred, or they may file electronically. Petitions for Violation of Injunction may also be filed by paper or electronically.

This portal provides a single point of information captured with an established electronic exchange to the 67 county's Clerk of Courts. Paper submissions to the Clerk of Courts may be scanned and uploaded to individual case management systems. Court orders are electronically submitted to the central repository that is managed by the Florida Department of Law Enforcement (FDLE). This repository then updates NCIC. The Florida Portal may be accessed here.

In 2018, the Florida Legislature created the Risk Protection Order that allows a law enforcement officer or agency to petition the court to temporarily prevent persons who are at high risk of harming themselves or others from possessing firearms or ammunition. The risk factors may include significant danger because of a mental health crisis or violent behavior. There is also a protection order against the exploitation of a vulnerable adult. Law Enforcement Agencies may petition by paper submission or electronically file through the Florida portal.

The Florida Department of Law Enforcement (FDLE) is working in an initiative called "eProtection Orders" to further automate the protection order process. This will build on FDLE's existing eWarrants platform. At this time, a workgroup has been established to work on system requirements. Domestic violence will be the first protection order developed followed by the risk protection order.

Some of the functionality of this automation would be to improve the connections between agency andbranch applications to better track the status of orders, allow for electronic notifications such as when protection orders are served or about to expire, and allow for a robust integrated platform where related information may be queried across different systems in different agencies and branches of government.

4.1.4. North Carolina's eCourts Civil Domestic Violence (ECCDV) System

North Carolina's eCourts Civil Domestic Violence (ECCDV) System allows petitioners in participating counties to electronically file applications for domestic violence protective orders and have their ex parte hearings remotely before a judge using WebEx.[27] Petitioners access the system from domestic violence service agencies, which can include law enforcement agencies.

As of January 2020, the ECCDV System is available in 14 counties in North Carolina. One of the counties, Cumberland County, includes Fort Bragg as a filing site accessible to petitioners. Fort Bragg is the largest military installation in

the world and the integration of the ECCDV system represents the first time that a civilian court has partnered with a military installation for the processing of civil domestic violence matters. In early 2019, the ECCDV System was linked to NCAware, North Carolina's statewide warrant repository system. This system integration ensures that law enforcement statewide has immediate access to domestic violence protective order documents in real time for purposes of enforcement. Local law enforcement officers no longer need to rely on the petitioner or a court clerk to provide them with a copy or a court clerk to provide them with a copy of the domestic violence protective order because it is available and accessible in NCAware.

Fort Bragg
Army Base is a filing site in North Carolina's eCourts Civil Domestic Violence System.

Protection order documents flow electronically to each partner in the process including clerks, judges, sheriff's deputies, law enforcement officers, advocates, petitioners, and whoever the petitioner designates to receive the documents. The documents are simply a digital version of the court file that is accessible to all partners at any time. Local law enforcement can rely on the integrity and accuracy of the electronic documents for enforcement because the digital files are updated immediately upon issuance of an order. Digital files within the ECCDV system can be accessed from any electronic device from any location that has internet access. Judges, clerks, advocates, litigants, and law enforcement therefore can view DVPO documents from anywhere in the state in real time.

Since the system launched, in combination with the use of videoconferencing for ex parte domestic violence cases, courtroom dockets flow more efficiently while ensuring matters are heard timely. One reason for this success is improvements in ex parte order service rates. For example, service rates in Durham County ranged from 4% to 14% before the ECCDV System launched in April 2017, and by February 2019, the service rate increased to 88%. Another success is the reduction of involuntary dismissals (i.e., matters that are dismissed because the petitioner fails to show up for the hearings) in all 14 of the ECCDV counties since their participation in system. For example, when Guilford County started using the ECCDV system in August of 2015 it recorded just over 800 involuntary dismissals. As of December 2019, Guilford County recorded just over 500 involuntary dismissals. This reduction is significant for survivor safety according to domestic violence agencies across the state, whose experiences suggest that involuntary dismissals are linked to repeat filings and domestic violence homicides.

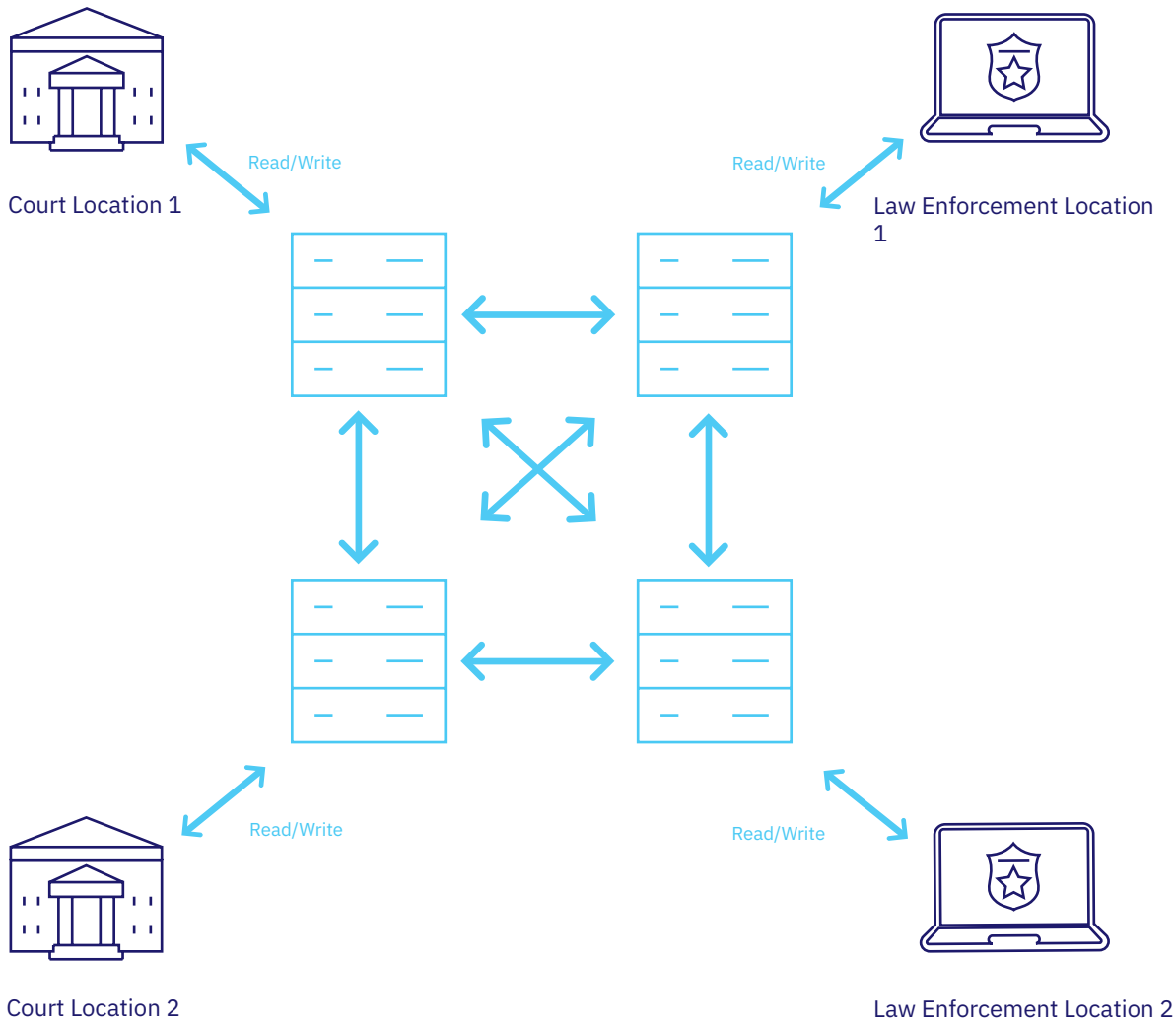
The ECCDV System has proven to be a sustainable model to increase access to file protective orders in North Carolina. The maintenance cost of the ECCDV System is combined with the cost of other e-filing systems in North Carolina and covered by the Administrative Office of the Courts. Additionally, partner agencies, such as domestic violence organizations, are urged to develop a sustainability plan for additional personnel and equipment to support petitioners prior to receiving the ECCDV system in their agencies. The court system leverages existing resources to utilize the ECCDV System at no additional cost.

4.2. Emerging Technologies and Approaches

Because there are multiple entities involved in the protection order process, the timeliness and accuracy of protection order availability and status have always been weaknesses of the overall system. Many emerging technologies provide opportunities to improve the reliability of protection order data.

4.2.1. Distributed Ledger Technology

Blockchain is one example of a Distributed Ledger Technology (DLT) that can provide key advantages to the protective order process as outlined in the IJIS Institute's Blockchain Task Force publication, "Use Case Assessment: Protective Orders." [28] Like many other technologies, any option that replaces a mainly paper process will likely improve the timeliness and accuracy of protective orders for all the actions of issuing, serving, and sharing/updating information through data exchange with NCIC.



The transactions in a distrubuted ledger system are written to multiple places. Unlike traditional data systems, they do not have a single central authority for the record, but rather each node contains an authoritative copy of the data. Users can read or write records through any node of the system.

Distributed Ledger Technology additionally assures an authoritative source and verifiable audit trail for protection orders. Some of this may be achieved by other technologies in various ways, but it is inherent in the concept of distributed ledgers. In addition, a properly designed implementation will provide varied access and security levels to properly protect data from unauthorized alteration.

The IJIS Institute's use case for protection orders re-envisions Missouri's decentralized paper-based petition process using a Distributed Ledger, like Blockchain, as an authoritative source of the order information that can be accessed by the petitioner, respondent, law enforcement, attorneys and the general public, where applicable. In contrast, the current paper process relies on faxes, emailed PDFs, or hand delivery. Individual Sheriffs' Offices determine how and when protective orders are entered into the Missouri Uniform Law Enforcement System, which then transmits orders to NCIC. Verifying critical information needed for enforcement, such as whether an order was served, what its terms are, and whether it is valid requires searches of multiple court and law enforcement sources.

4.2.2. Event-Based Messaging, Replication and Streaming

Some courts are using traditional messaging technologies, such as standard messaging queues, to transmit orders to their state police repositories. Traditional messaging provides for near "real-time transmission" of orders from the courts to the state police for packing and transmission to NCIC. When implemented from a case management system or e-filing system, messaging can provide more reliability in that it involves semi-persistent queues that can be monitored and where data transmission can be retried and monitored.

In addition, modern database replication tools have become more advanced and include more adaptors to connect disparate databases, such as Oracle and SQL Server. Since these also rely on database log transactions, they offer the opportunity for less human intervention and more "near real-time" transmission. [29]

Streaming technologies involve non-standard message queues such as Kafka (Confluent) [30] and/or No-SQL [31] databases to transmit and store database log transactions in native format. These technologies offer promise in "near real-time," change data capture that provides for incremental replication of data from a source to a destination without the need to write custom adapters. These also offer semi-persistent data that can be used for transmission retries and monitoring.[32]

CHAPTER 5

Conclusion

5. Conclusion

Technology has been a powerful tool for advancing the availability and impact of protection orders on the safety and well-being of domestic violence survivors. Protection order processes in many states have evolved from decentralized paper-based systems to primarily automated systems that more efficiently transmit accurate orders to state and federal repositories. These repositories are important resources because they provide the electronic record needed to verify the existence and validity of a protection order when a physical copy is not available. They also offer critical information about possible histories of abuse by defendants to judges, prosecutors, law enforcement officers, and advocates as they carry out their responsibilities to make informed decisions and keep victims safe.

State protection order repositories are most effective when they:

- Include more comprehensive information that facilitates service and enforcement of all the protections a court has ordered, such as emergency and ex parte orders, notice of service, stalking and sexual assault orders, elder abuse orders, criminal protection orders, child custody orders, divorce decrees, and criminal pretrial release and sentencing orders.
- Are developed in collaboration with a broad range of stakeholders, including advocates and allied community-based service providers.
- Are governed by policies that set standards for timeliness, accuracy, data quality, and security.
- Follow technology standards for designing, implementing, and maintaining data exchanges.
- Require standardized forms with sufficient numeric identifiers to allow entry into the NCIC POF.
- Capitalize on cloud-based technologies that offer greater scalability and resiliency to outages and other transmission disruptions.

Advanced technologies allow courts to offer online petitioning and electronic filing processes for protection orders. A few states have designed and implemented web-based technologies for obtaining protection orders with survivor safety and system efficiency as the paramount objectives.

To maximize the ability of survivors to obtain the safety protections and legal remedies available through protection orders, states and local courts should:

- Streamline processes for obtaining a protection order, whether in-person or remotely.
- Widen accessibility through web-based petitioning and issuance of orders.
- Consider the benefits of allowing survivors to electronically file protection order petitions.
- Collaborate with advocates, law enforcement, and other stakeholders to ensure that online petitioning and e-filing systems incorporate user-friendly interfaces, easy exit functions, online security measures, safety planning, and guidance from advocates on the consequences of filing a petition.

As new technologies continue to emerge, they will offer justice system stakeholders greater opportunities to imagine and implement systems to respond more effectively to domestic violence, sexual assault, stalking, and dating violence. The value of technology has been made imminently clear during the 2020 COVID-19 pandemic. It will continue to be an important way to maintain lifelines for survivors during normal times and future challenges caused by other pandemics, natural disasters, and the effects of climate change.

This publication was produced by the National Center for State Courts (NCSC) in partnership with the National Center on Protection Orders and Full Faith and Credit (NCPOFFC) and the Center for Court Innovation (CCI). The authors are Susan Keilitz, Jannet Okazaki, Barbara Holmes, and Shauna Strickland (NCSC), Monica Player (NCPOFFC), Robyn Mazur and Wai Khoo (CCI), in collaboration with NCSC staff Alice Allred, Caisa Royer, Shelley Spacek Miller, Kathryn Genthon, Jackie Gilbreath, Emily Montalvo, and Ivy Garrenton.

Endnotes

1 In 2018, forty-nine states, the District of Columbia, Guam, and Puerto Rico reported a total caseload of over 956,586 civil protection/restraining orders. (Court Statistics Project, National Center for State Courts. 2020. Data accessed 5/8/2020). For a broad range of resources on protection orders see the National Center on Protection Orders and Full Faith and Credit and the National Council of Juvenile and Family Court Judges Civil Protection Orders Online Resources.

2 The NCIC POF facilitates enforcement of valid protection across state and tribal jurisdictions, as required by the Full Faith and Credit provisions of the Violence Against Women Act, and is a key source of information tapped by the National Criminal Background Check System (NICS) to prevent illegal firearms purchases.

3 See, State Progress in Record Reporting for Firearm-Related Background Checks. The authors report that at the end of 2014, state repositories contained over 2.1 million protection orders, while only 1.4 million were entered in the NCIC POF and NICS.

4 https://dictionary.cambridge.org/us/dictionary/english/repository

5 https://www.lexico.com/en/definition/repository

6 https://nnedv.org/mdocs-posts/protection-order-registries-databases/

7 Battered Women Justice Project's (BWJP) State and Territorial Protection Order Registry/Database and Registration Statutes.

8 Information derived from State and Territorial Protection Order Registry/Database and Registration Statutes and SEARCH's Survey of State Criminal History Information Systems, 2016: A Criminal Justice Information Policy Report.

9 See State and Territorial Protection Order Registry/Database and Registration Statutes, note 7.

10 Inclusion of an order in a state protection order repository does not ensure that the order meets the definition of a protection order for the purposes of entry into the NCIC POF. See 28 U.S.C. § 534 (f)(3)(B).

11 N.J. Stat. § 2C:25-34

12 Survey of State Criminal History Information Systems, 2016: A Criminal Justice Information Policy Report, pg. 4.

13 Miss. Code Ann. § 93-21-25(2)

14 https://www.oreilly.com/library/view/designing-data-intensive-applications/9781491903063/

15 The NCIC database was launched by the FBI on January 27, 1967. It consists of 21 files; the Protection Order File (POF) is one of 14 persons files. For statutory authority to maintain the NCIC POF see 28 USCS § 534.

16 The nine states are Alabama, Ala. Code § 30-5-8(a)(3); Arizona, Ariz. Rev. Stat. § 13-3602(P) (Effective January 1, 2020); Georgia, Ga. Code Ann. § 19-13-52(d); Kansas, K.S.A. § 60-3112 (a); Mississippi, Miss. Code Ann. § 93-21-25 (2); Montana, Mont. Code Ann. § 40-15-303 (1); North Dakota, N.D. Cent. Code § 12.1-31.2-01(9); North Carolina, N.C. Gen. Stat. § 50B-3(d); and Oregon, Or. Rev. Stat. Ann. § 107.720(1)(a). Puerto Rico also mandates entry into NCIC, See, 8 L.P.R.A. § 675(b) Note, Oklahoma suggests entering orders into the NCIC, Okla. Stat. Ann. Tit. 22, § 60.5 (B) (Effective November 1, 2019)

17 See Survey of State Criminal History Information Systems, 2016: A Criminal Justice Information Policy Report, Table 4a -Entry of state protection order information onto FBI-NCIC and record counts, 2016. The Tribal Law and Order Act provided tribal law enforcement agencies access and entry into NCIC. See INDIAN ARTS AND CRAFTS AMENDMENTS ACT OF 2010; TRIBAL LAW AND ORDER ACT OF 2010, 111 P.L. 211, 124 Stat. 2258; See also 28 USCS § 534(d),(f). Some tribes have entered into agreements with state or local jurisdictions to obtain access to NCIC. In August 2015, the Department of Justice launched the Tribal Access Program for National Crime Information (TAP) to provide tribal law enforcement access to NCIC, Currently, 50 tribal jurisdictions are participating in TAP. See https://www.justice.gov/tribal/tribal-access-program-tap

18 See NCIC Operating Manual Introduction Chapter, Section 3.4. Validation. Validation means that the entering agency must confirm that the record it is sending is complete, accurate, and still active.

19 The NCIC POF defines the term "protection order" as: (A) any injunction, restraining order, or any other order issued by a civil or criminal court for the purpose of preventing violent or threatening acts or harassment against, sexual violence, or contact or communication with or physical proximity to, another person, including any temporary or final order issued by civil or criminal courts whether obtained by filing an independent action or as a pendente lite order in another proceeding so long as any civil order was issued in response to a complaint, petition or motion filed by or on behalf of a person seeking protection; and (B) any support, child custody or visitation provisions, orders, remedies or relief issued as part of a protection order, restraining order or injunction pursuant to state, tribal, territorial, or local law authorizing the issuance of protection orders, restraining orders or injunctions for the protection of victims of domestic violence, sexual assault, dating violence, or stalking. See 28 USCS § 534 (f)(3)(B). The Full Faith and Credit provision of the Violence Against Women Act uses a similar definition. See 18 U.S.C. §2266(5).

20 See NCIC Operating Manual- Protection Order File Entry, Section 2.2; 2.3.

21 See NCIC Operating Manual – *Introduction Chapter, Section 3.5 Hit Confirmation Procedures*; NCIC Operating Manual- Protection Order Chapter, Section 5.6. Procedures for Handling a Hit

22 See NCIC Operating Manual- Protection Order File, Inquiry, Section 5.6.

23 See "NCIC Policy Provides Guidance for Electronic Records as the Source Documentation for NCIC Records" section of State Progress in Record Reporting for Firearm-related Background Checks: Protection Order Submissions.

24 The portal e-filing service provider is accessible at https://public.courts.in.gov/porefsp#/. The information page geared toward pro se petitioners is accessible at https://www.in.gov/judiciary/5538.htm

25 The Arizona Supreme Court collaborated with the Arizona Criminal Justice Commission (ACJC) to build the web portal. The project is supported by the court's share of Arizona's STOP Grant. The IT Division of the Arizona Administrative Office of the Court (AOC) directed a web developer in building the petition and court clerk portals, as well as the service portal through which law enforcement can document service and provide notice to plaintiffs when their orders have been served.

26 During the COVID-19 pandemic, plaintiffs are instructed to call the court for further instruction. Courts have been conducting ex parte hearings by telephone and or video.

27 The project that oversees the ECCDV system is a partnership between the Administrative Office of the Courts (AOC), law enforcement, and local domestic violence agencies. It is funded through an Office on Violence Against Women Improving Criminal Justice Response to Sexual Assault, Domestic Violence, Dating Violence, and Stalking Program Grant.

28 Use Case Assessment: Protective Orders. Jim Kita, Tom Messerges, Anil Sharma, Anne Thompson, Steven White. Retrieved from https://cdn.ymaws.com/ijis.site-ym.com/resource/collection/93F7DF36-8973-4B78-A190-0E786D-87F74F/IJIS_Use_Case_Protective_Orders_FINAL.pdf

29 See "Streaming Data Capture, A Foundation for Data Architecture by Kevin Petrie, Dan Potter & Itamar Ankorian, O'Reilly Media, 2019.

30 See https://www.confluent.io/

31 See https://en.wikipedia.org/wiki/NoSQL

32 See "Kafka, The Definitive Guide, Real-time Data and Stream Processing at Scale," Neha Narkhede, Gwen Shipiro, Todd Palino, O'Reilly Media, 2017.