# VENDOR REQUIREMENTS RE: E-SUBMISSION SYSTEMS

County Clerks have an option to provide an electronic submission system for petitioners to submit their protection orders. There are many private vendors that provide these systems and services. Clerks will need to research and analyze which private vendor system can integrate best with their local document management systems and court electronic systems. The following list of generic requirements is provided to assist clerks in determining what to look for when researching or contracting with potential private vendors to provide electronic filing for protection orders.

## USER EXPERIENCE:

- Provide electronic submissions for all six types of protection orders
- Capability to be used and accessed via smart phone
- Allow for saving of partially completed filings
    - Notify users how long they have to work on draft documents
    - Provide an estimate for how long it will take to complete the documents
- Provide Emergency Escape button to close the browser window and clear browser history with one click
- Guide petitioners through the process of completing protection order documents in an interactive, easy to use, plain language, Q&A format
- Provide users with the ability to download forms and questions in advance, including drafts, along with an advisory notice, e.g. "if you download this, it will be on your computer"
- Integrate advocate access
- Include resources for legal assistance for *pro se* petitioners
- Provide required notifications for all parties, including local law enforcement, by email
- Allow parties to opt-out of status notifications to ensure that perpetrators do not inadvertently become aware of a victim's attempt to obtain protection

## COURT/CLERK OPERATIONS:

- Provide timely notification of new filing to include alerts to staff that a protection order has been submitted
- Check for viruses, provide for IT processes protecting against firewall, spam, clutter, or other potential barriers to receiving protection orders submitted electronically
- Provide required notifications for all parties, including local law enforcement, by email
- Allow for electronic submission of Returns of Service by law enforcement
- Accommodate electronic service of protection orders to respondents by law enforcement
- Requirement that vendor is responsible for system updates when laws and procedures change
- Capacity to autofill forms that are compatible with state forms
- Allow for simple submission of digital evidence, e.g. uploading attachments

## PRIVACY CONSIDERATIONS:

Cybersecurity requires ongoing care and attention to maintain, and most controls come down to processes and people. Security and privacy risks associated with working with vendors include:

- Loss of control
- Lack of information about data impacted by a cyber event
- Compromise of your own system

- Service availability, business continuity, disaster recovery
- Reputational, compliance, legal, and financial risks
- Many third-party applications will re-sell data
- Compliance with any policies, external regulations, or law

To mitigate these risks, what follows are recommendations, including practices and provisions, to use in contracts with private vendors who may have access to court users' information:

- Use contract templates and standards
- Centralize documentation, keep files organized
- Require background check for vendors
- Assess vendor security and require evidence of a mature program, e.g. SOC 2 Type 2
- Include contract provisions regarding cyber incident notification to courts and to court users whose data may have been compromised:
    - Notification within certain timeframe
    - Delegate a contact for notification and keep that information up-to-date
    - Determine whether the court or vendor will notify the court user
    - Involve advocates in the notification processes
    - Creation of user profiles should include safe notification methods for cyber incidents
- Require encryption of data that is industry standard and subject to audit
- Require multi-factor authentication for accessing confidential data
- Include contract provisions regarding data retention:
    - No personal identifying information about litigants should be stored beyond the use of it to pass from vendor to courts
    - Plan for contingencies, e.g.
        - What happens if the vendor stops supporting the product?
        - Is vendor data subpoenable?
    - Use least privilege and expiring permissions
    - Include timeframes for how long data is kept. Consider acceptable timeframes that are a reasonable compromise between data security and reasonable user experience (e.g. petitioner not needing to complete documents in one sitting)
    - Where is data stored
    - How is data destroyed
- Include contract provisions regarding data privacy
    - Prohibit the use of data for marketing purposes
    - Build privacy audits into contract language, including who will conduct, how often, and who will pay
    - Limit access to data, e.g. pre-approval or background check required, emergency clause