JUDICIAL COUNCIL OF CALIFORNIA

455 Golden Gate Avenue · San Francisco, California 94102-3688
www.courts.ca.gov

REPORT TO THE JUDICIAL COUNCIL

For business meeting on: September 20, 2018

Title
Rules and Forms: Remote Access to Electronic Records

Rules, Forms, Standards, or Statutes Affected
Adopt Cal. Rules of Court, rules 2.515–2.528 and 2.540–2.545; amend rules 2.500–2.503

Recommended by
Information Technology Advisory Committee
Hon. Sheila F. Hanson, Chair

Agenda Item Type
Action Required

Effective Date
January 1, 2019

Date of Report
August 31, 2018

Contact
Andrea L. Jaramillo, 916-263-0991
andrea.jaramillo@jud.ca.gov

Executive Summary

The Information Technology Advisory Committee recommends that the Judicial Council adopt a new set of rules of court governing remote access to electronic records by parties, parties' attorneys, court-appointed persons, legal organizations, qualified legal services projects, and government entities. This proposal advances a major initiative of the judicial branch's *Tactical Plan for Technology 2017–2018* to develop rules "for online access to court records for parties and justice partners." These changes will facilitate the trial courts' existing relationships with these persons and entities, and will provide clear authority for the trial courts to provide them with remote access to electronic court records. The committee also recommends limited amendments to the existing public access rules to bring them into conformance with the new rules.

Recommendation

The Information Technology Advisory Committee recommends that the Judicial Council, effective January 1, 2019:

1. Amend chapter 2 of division 4 of title 2 of the California Rules of Court to split the chapter into the following four articles to organize the chapter topically and accommodate the new proposed rules:
   - Article 1. General Provisions
   - Article 2. Public Access
   - Article 3. Remote Access by a Party, Party's Attorney, Court-Appointed Person, or Authorized Person Working in a Legal Organization or Qualified Legal Services Project
   - Article 4. Remote Access by Government Entities
2. Adopt rules 2.515–2.528 and 2.540–2.545 to allow remote access to electronic records by specified persons.
3. Amend rules 2.500–2.503 to expand the scope of the chapter and define new terms relevant to remote access.

The text of the new and amended rules is attached at pages 17–43.

Relevant Previous Council Action

The Judicial Council adopted the public access rules effective July 1, 2002, and has amended them periodically since then. The last amendments were in 2013. The public access rules contain provisions for access to electronic court records both in the courthouse and remotely.

Analysis/Rationale

The existing rules governing electronic access to trial court records are in chapter 2 of division 4 of title 2 of the California Rules of Court (hereafter chapter 2). Chapter 2's rules currently apply "only to access to court records by the public" and limit what is remotely accessible by the public to registers of actions, calendars, indexes, and court records in specific case types. (Cal. Rules of Court, rules 2.501(b), 2.503(b).) The rules in chapter 2 "do not limit access to court records by a party to an action or proceeding, by the attorney of a party, or by other persons or entities that are entitled to access by statute or rule." (Cal. Rules of Court, rule 2.501(b).) Because courts are moving swiftly toward making remote access to records available to these persons and entities, it is important to provide authority and guidance for the courts and others on these expanded forms of remote access.

Because chapter 2 limits only *public* remote access, a gap exists in the rules with respect to persons and entities that are not the public at large, such as parties, parties' attorneys, and justice partners. Courts have had to fill this gap on a piecemeal, ad hoc basis. Under the leadership of the Information Technology Advisory Committee (ITAC), nine advisory committees[1] formed the Joint Ad Hoc Subcommittee on Remote Access to develop a remote access rules proposal

[1] The committees include the Advisory Committee on Providing Access and Fairness, Appellate Advisory Committee, Civil and Small Claims Advisory Committee, Criminal Law Advisory Committee, Family and Juvenile Law Advisory Committee, ITAC, Probate and Mental Health Advisory Committee, Traffic Advisory Committee, and Tribal Court–State Court Forum.

applicable to parties, their attorneys, and justice partners. The purpose of the proposal is to create a new set of rules applicable statewide governing remote access to electronic records to provide more structure, guidance, and authority for the courts. The proposal neither creates a right to remote access nor provides for a higher level of access to court records using remote access than one would get by viewing court records at the courthouse.

The proposal restructures and expands the scope of chapter 2. It breaks the chapter into four articles to cover access not only by the public, but also by parties, their attorneys, legal organizations, court-appointed persons, and government entities. In brief, the new structure consists of:

- **Article 1. General Provisions.** Rules 2.500–2.502.
  This article builds on existing rules, covers broad concepts on access to electronic records, and expands on the definitions of terms used in chapter 2.
- **Article 2. Public Access.** Rules 2.503–2.507.
  This article consists of the existing public access rules, with minor amendments.
- **Article 3. Remote Access by a Party, Party's Attorney, Court-Appointed Person, or Authorized Person Working in a Legal Organization or Qualified Legal Services Project.** Rules 2.515–2.528.
  This new article covers remote electronic access by those listed in the article's title.
- **Article 4. Remote Access by Government Entities.** Rules 2.540–2.545.
  This new article covers remote electronic access by government entities.

Article 1. General Provisions

This article builds on existing rules and broadens the scope of chapter 2 beyond public access.

Rule 2.500. Statement of purpose. The proposal amends the rule to expand the scope of the chapter on access to electronic trial court records to include remote access by parties, parties' attorneys, legal organizations, court-appointed persons, and government entities. Language on access to confidential and sealed records is stricken from subdivision (c) because the rules allow access to such records by those who would be legally entitled to access them. For example, although the public at large may not be legally entitled to access a sealed record under any circumstance, a party who could access a sealed record at the courthouse would be able to access that record remotely under the new rules.

Rule 2.501. Application, scope, and information to the public. The proposal amends subdivision (a) to provide more explanation of what types of records are and are not within the scope of chapter 2's provisions. Chapter 2 governs access only to "court records" as defined in the chapter and not to any other type of record that is not a court record. The proposal also adds an advisory committee comment providing additional details about the limitation.

The proposal amends subdivision (b) by replacing the existing language with a new provision. Because the new rules expand the scope of remote access by allowing certain persons and entities remote access not allowed to the public, the new provision requires courts to provide

information to the public on who may access their court records under the rules of the chapter. Courts may provide the information by linking to information that will be posted publicly on *www.courts.ca.gov* and may supplement that with guidance in plain language on their own websites.

Rule 2.502. Definitions. The proposal expands on the definitions found in this rule by adding new terms applicable to the expanded scope of chapter 2. The proposal also makes minor edits to the existing definitions. Most of the definitions are discussed in other sections of this report where the terms are applicable. For example, the meaning of "government entity" is discussed below in conjunction with article 4, which covers remote access by government entities.

One item of note, however, is that within the scope of chapter 2, a "person" is defined as a natural human being. The reason is that the remote access rules are highly person-centric when describing who can remotely access what. Ultimately, the new rules contemplate that a natural human being will be remotely accessing electronic court records, and the rules identify which natural human beings are authorized to do so. This is not to say that the organizational entities that are legal persons, such as corporations, cannot have access, but they must do so through natural human beings.

Article 2. Public Access

Article 2 largely retains the existing public access rules found in rules 2.503 through 2.507. Rule 2.503 is the only one with substantive amendments and ITAC's proposed amendments are minor. They clarify that the rules in this article apply only to access to electronic records by the public. The amendments also make a technical change to the enumerated list of electronic records to which a court must provide for electronic access by the public. Under rule 2.503(b), all court records in civil cases must be available remotely, if feasible, "except those listed in (c)(1)–(9)." Subdivision (c) was amended effective January 1, 2012, with an addition of a tenth case type (in subd. (c)(10)), but there was no corresponding amendment to the reference to the list in subdivision (b). The omission was accidental and the proposal corrects the incongruity. The proposal also makes a technical correction consistent with the rest of the rules by adding "court" to "all records" so that it states "all court records."

The Civil and Small Claims Advisory Committee is concurrently recommending a substantive amendment to rule 2.503 under the council report titled, "Protective Orders: Entry of Interstate and Tribal Protective Orders, Canadian Protective Orders, and Gun Violence Restraining Orders into CLETS." The amendment adds an eleventh case type to 2.503(c)—for gun violence prevention proceedings—requiring yet another change to both the above-mentioned cross-reference in rule 2.503(b) and the list of case types under 2.503(c). To reconcile all of the amendments to rule 2.503 recommended by both the Civil and Small Claims Advisory Committee and ITAC, the committees have jointly proposed one consolidated, amended rule 2.503 for the council's consideration.

Article 3. Remote Access by a Party, Party's Attorney, Court-Appointed Person, or Authorized Persons Working in a Legal Organization or Qualified Legal Services Project

This article contains new rules to cover remote access by those listed in the article's title. Each of these types of users is discussed below. The rules make clear that article 3 is not intended to limit remote electronic access available under article 2 (the public access rules). Accordingly, if a user could have remote access to a court record under article 2, that user may do so without meeting the requirements of article 3. The rules under article 3, as with the public access rules, require courts to provide remote electronic access only if it is feasible to do so. Finally, the rules in article 3 include requirements for identity verification, security of confidential information, and additional conditions of access.

The rules in article 3 have occasional, intentional repetition to ensure that they are clear to a person accessing the records. For example, under rule 2.515—the rule explaining the scope of article 3—there is a provision stating that the rules do not limit the access available under article 2. This statement is repeated in rule 2.517, which is the rule applicable to parties, so that parties who may not be versed in reading rules of court do not have to search to understand that their ability to gain public access in article 2 is not limited by rule 2.517.

Rule 2.515. Application and scope. This rule provides an overview of the scope of article 3 and who may access electronic records under that article.

Rule 2.516. Remote access to extent feasible. This rule requires courts to allow remote access to electronic records by the types of users identified in rule 2.515. This requirement is similar to the public access requirement in rule 2.503. The advisory committee comment recognizes that financial means, technical capabilities, and security resources may impact the feasibility of providing remote access.

Rule 2.517. Remote access by a party. This rule allows broad access to remote electronic court records by a *person* (defined as a natural human being in the definitions in rule 2.502) when accessing electronic records in actions or proceedings in which that person is a party. The reason for this limitation is that a natural human being must ultimately be the one who accesses the records. Parties that are not natural human beings can still gain access to their own electronic records but must do so through an attorney or other "authorized person" under the other rules in article 3 or, for certain government entities, article 4.

Rule 2.518. Remote access by a party's designee. This rule allows a party who is a person to designate other persons to access the party's electronic records. The rule allows the party to set limits on the designee's access, such as to specific cases or for a specific period of time. In addition, the designee may have only the same access to a party's electronic records that a member of the public would be entitled to if he or she were to inspect the party's court records at the courthouse. For example, if a court record is sealed and the designee is not entitled to view the court record at the courthouse, the designee cannot remotely access the electronic record. In addition, regardless of whether there are publicly accessible court records at the courthouse for criminal, juvenile justice, or child welfare records, the party's designee rule does not allow

remote access to those particular records. Criminal electronic records were exempted because of the sensitivity of the information, combined with the potential for a person to be subject to pressure from gangs to designate gang members to be allowed remote access to the person's criminal records. Juvenile justice and child welfare electronic records were exempted because of the sensitivity of the information, combined with the fact that counsel are typically involved and attorneys for minors and parents can gain access under other rules.

The rule states the basic terms of access, though additional terms may be set by the court in a user agreement. The rule does not prescribe a particular method for establishing a designation because the method may depend on the preferences and technical capabilities of individual courts.

Rule 2.519. Remote access by a party's attorney. This rule allows a party's attorney to remotely access electronic records in the party's actions or proceedings. Remote access may also be provided to an attorney appointed by the court to represent a party pending the final order of appointment. Attorneys may also potentially gain access under rule 2.518, in which case the provisions of that rule would apply.

Attorneys of record should already be known to the court for remote access purposes. The rule also allows courts to provide remote access to an attorney who is not the attorney of record in an underlying proceeding but who may nonetheless be assisting a party. For example, he or she may be providing undisclosed representation and assisting a party with limited aspects of the case, such as document preparation, without becoming the attorney of record.

Subdivision (c) requires an attorney who is not of record to obtain the party's consent to remotely access the party's court records and represent to the court in the remote access system that he or she has obtained the party's consent. This process provides a mechanism for an attorney not of record to be known to the court and provides the court with assurance that the party has agreed to allow the attorney to remotely access the party's electronic records. The proposed rule also states the basic terms of access.

As with the other rules, the level of access under this rule is limited to what a member of the public could get if he or she went to the courthouse. An undisclosed attorney providing limited scope representation (as opposed to an attorney providing noticed limited scope representation) would only be able to remotely access electronic records that the public could access at the courthouse.

Rule 2.520. Remote access by persons working in the same legal organization as a party's attorney. Because attorneys often work with other attorneys and legal staff, proposed rule 2.520 allows remote access by persons "working in the same legal organization" as a party's attorney. Both "legal organization" and "working in" are broad in scope. Under the definitions in amended rule 2.502, "legal organization" means "a licensed attorney or group of attorneys, nonprofit legal aid organization, government legal office, in-house legal office of a nongovernmental organization, or legal program organized to provide for indigent criminal, civil, or juvenile law

representation." Those working in the same legal organization as a party's attorney may include partners, associates, employees, volunteers, and contractors. The goal is to capture the full range of ways that attorneys may be working together and with others to provide representation to a party.

Under the rule, a party's attorney can designate other persons working in the same legal organization to have remote access, and the attorney must certify that those persons are working in the same legal organization and assisting the attorney with the party's case. The rule does not require certification to take any specific form. The rule also states the terms of access.

Rule 2.521. Remote access by a court-appointed person. In some proceedings, the court may appoint someone to participate in a proceeding or represent the interests of someone who is not technically a "party" to a proceeding (e.g., a minor child in a custody proceeding). The rule provides common examples of court-appointed persons but does not limit remote access to those examples. The proposed rule also states the basic terms of access.

Rule 2.522. Remote access by persons working in a qualified legal services project providing brief legal services. This rule allows remote access to electronic records by persons "working in" a "qualified legal services project" providing "brief legal services." The rule contemplates legal aid programs offering individuals limited, short-term services for their court matters. "Brief legal services," for purposes of chapter 2, is defined in rule 2.502 as "legal assistance provided without, or before, becoming a party's attorney. It includes giving advice, having a consultation, performing research, investigating case facts, drafting documents, and making limited third party contacts on behalf of a client."

The rule applies only to qualified legal services projects as defined in Business and Professions Code section 6213(a). The purpose of this limitation is to ensure that the organizations are bona fide entities subject to professional standards. The definition of "qualified legal services project" under Business and Professions Code 6213(a) is:

> (1) A nonprofit project incorporated and operated exclusively in California that provides as its primary purpose and function legal services without charge to indigent persons and that has quality control procedures approved by the State Bar of California.
>
> (2) A program operated exclusively in California by a nonprofit law school accredited by the State Bar of California that meets the requirements of subparagraphs (A) and (B).
>
> (A) The program shall have operated for at least two years at a cost of at least twenty thousand dollars ($20,000) per year as an identifiable law school unit with a primary purpose and function of providing legal services without charge to indigent persons.
>
> (B) The program shall have quality control procedures approved by the State Bar of California.

When an attorney from a qualified legal services project becomes a party's attorney and offers services beyond the scope contemplated under this rule, the remote access rules for a party's attorney would also provide a mechanism for access, as could the party's designee rule. This proposed rule also states the basic terms of access.

Rule 2.523. Identity verification, identity management, and user access. This rule requires a court to verify the identity of a person eligible to have remote access to electronic records under article 3 except for a party designee granted access under rule 2.518. This will allow the court to know that persons seeking access are who they say they are. There is an exception for party designees granted access under rule 2.518 because unlike remote access by other third parties under article 3, the party's designee rule allows the party to directly communicate with the court about who should have remote access to the party's electronic records. The parties themselves are able to control who gains access under the party's designee rule, which mitigates concerns about unknown third persons gaining unauthorized remote access.

Subdivision (b) describes the responsibilities of the court to verify identities and provide unique credentials to users. The rule does not prescribe any particular mechanism for identity verification or credentials because the best solutions may differ from court to court. A court could perform identity verification itself or, under subdivisions (d) and (e), rely on other entities to perform the verification. Subdivision (c) describes the responsibilities of users who seek remote access as follows: to provide necessary information for identity verification, to consent to conditions of access, and to obtain authorization by the court to have remote access to electronic records. Subdivision (d) describes responsibilities of legal organizations and qualified legal services projects to verify the identity of users it designates and notify the court when a user is no longer working in the legal organization or qualified legal services project. Subdivision (e) makes it clear that courts may enter into contracts or participate in statewide master agreements for identity verification, identity management, or access management systems.

Rule 2.524. Security of confidential information. This rule requires that when information in an electronic record is confidential by law or sealed by court order, remote access must be provided through a secure platform and transmissions of the information must be encrypted. As with the identity verification requirements, courts may participate in contracts for secure access and encryption services.

Rule 2.525. Searches; unauthorized access. This rule allows users who have remote access under article 3 to search for records by case number or case caption. The court must ensure that only authorized users are able to remotely access electronic records. The limitation on searches by case number or case caption is intended to prevent inadvertent unauthorized access. However, recognizing that unauthorized access may still occur, the rule includes measures for the user to take in that event.

Rule 2.526. Audit trails. The purpose of this rule is to encourage courts to have the ability to generate audit trails that document who remotely accessed electronic records, under whose authority the user gained access, what electronic records were accessed, and when the record was

accessed. The audit trail is a tool to assist the courts in identifying and investigating any potential issues or misuse of remote access. The rule also encourages the courts to provide limited audit trails to authorized users who are remotely accessing remote records under article 3. A limited audit trail would show the users who remotely accessed electronic records in a particular case but would not identify which specific electronic records were accessed. This limited view protects confidential information while still providing users with a tool to identify potential unauthorized remote access.

Rule 2.527. Additional conditions of access. This rule requires courts to impose reasonable conditions on remote electronic access to preserve the integrity of court records, prevent the unauthorized use of information, and limit possible legal liability. The court may require users to enter into user agreements defining the terms of access, providing for compliance audits, specifying the scope of any liability, and providing for sanctions for misuse up to and including termination of remote access. The court may require each user to submit a signed, written agreement, but the rule does not prescribe any particular format or technical solution for the signature or agreement.

Rule 2.528. Termination of remote access. This rule makes clear that remote access to electronic records is a privilege and not a right and that courts may terminate any grant of permission for remote access.

Article 4. Remote Access by Government Entities

Article 4 contains new rules to cover remote access by persons authorized by government entities for legitimate governmental purposes. Under the definitions in amended rule 2.502, "government entity" means "a legal entity organized to carry on some function of the State of California or a political subdivision of the State of California. A government entity is also a federally recognized Indian tribe or a reservation, department, subdivision, or court of a federally recognized Indian tribe."

Rule 2.540. Application and scope. This rule identifies which government entities may have remote access to which types of electronic records and is geared toward government entities that have a high volume of business before the court with respect to certain case types. To anticipate all needs across California's 58 counties and superior courts is impossible; thus, the rule includes a "good cause" provision under which a court may grant remote access to electronic court records to additional government entities in particular case types beyond those specifically identified in the rule. The standard for good cause is that the government entity requires access to the electronic records in order to adequately perform its statutory duties or fulfill its responsibilities in litigation.

The rule does not preclude government entities from gaining access to court records through articles 2 and 3, nor does it grant higher levels of access to court records than currently exists. Rather, as with the rules under article 3, it provides for remote access only to electronic records that the government entity would be able to obtain if its agents appeared at the courthouse to inspect the records in person.

Rule 2.541. Identity verification, identity management, and user access. This rule largely mirrors rule 2.523 and describes the responsibilities of the court, authorized persons, and government entities for identity verification and user access. The rule also makes it clear that courts may enter into contracts or participate in statewide master agreements for identity verification, identity management, or access management systems.

Rule 2.542. Security of confidential information. This rule largely mirrors rule 2.524 in requiring secure platforms and encryption of confidential or sealed electronic records and in authorizing courts to participate in contracts for secure access and encryption services.

Rule 2.543. Audit trails. This rule mirrors rule 2.526.

Rule 2.544. Additional conditions of access. This rule mirrors rule 2.527.

Rule 2.545. Termination of remote access. This rule mirrors rule 2.528.

Policy implications

ITAC anticipates that amendments to the rules will be necessary in the future. In particular, the committee expects the rules encouraging the use of audit trails—rules 2.526 and 2.543—to become mandatory. As circulated, the audit trail rules were mandatory, but the committee sought specific comments on whether the requirement would present a challenge and whether there were more feasible alternatives. The Joint Technology Subcommittee of the Trial Court Presiding Judges Advisory Committee and Court Executives Advisory Committee, joined by the Superior Court of Placer County, recommended that the audit trail requirement be nonmandatory. The Joint Technology Subcommittee commented, "The current mandatory language may result in a court being prohibited from providing any electronic access even with the ability to do so, if the court does not have the ability to provide the required audit trail." A goal of the rules proposal is to facilitate current use of remote access rather than inhibit it. Accordingly, ITAC agreed that the audit trail rules should be nonmandatory for now. However, ITAC recognized the importance of having the ability to audit and added an advisory committee comment that audit trails would become a requirement in the future. ITAC will circulate amendments in another rule cycle to seek feedback from the courts on potential dates by which the rules should be amended to be mandatory.

Comments

This rules proposal circulated for public comment from April 9 to June 8, 2018. Thirteen commenters responded to the invitation to comment. The following topics generated the most interest:

- Feasibility of providing remote access (rule 2.516);
- Allowing a party to designate users to remotely access the party's electronic records (rule 2.518);
- Allowing an undisclosed attorney to remotely access a party's electronic records (rule 2.519(c));

- Allowing a qualified person from a qualified legal services project to remotely access a party's electronic records (rule 2.522);
- Requiring courts to verify the identities of remote access users (rule 2.523);
- Audit trails documenting information about user access (rules 2.526 and 2.543); and
- Provisions for remote access by Department of Child Support Services and local child support agencies (rule 2.540).

The comments on these topics are discussed below. For all other comments, please see the chart of comments at pages 44–91.

Comments on rule 2.516. This rule requires the courts to provide remote access to users under article 3 if it is feasible to do so. The Joint Technology Subcommittee, joined by the Placer court, commented, "[A]s written it is unclear whether it is ITAC's intent that courts refrain from moving forward with *any* part of the remote access options until they can move forward with *all* of the options." (Italics added.) The commenters recommended additional clarification in the rule or in an advisory committee comment. ITAC did not intend article 3 to be an "all-or-none" proposition because it may not be feasible for a court to add all the users outlined in rule 2.515 at once. The committee added an advisory committee comment to clarify this.

The Joint Technology Subcommittee, joined by the Placer court, commented that rule 2.519(c), which governs remote access by attorneys who are not attorneys of record, presents a significant security risk. In response, the committee added "security resources" to the advisory committee comment to rule 2.516 as a consideration for feasibility. Thus, if it is not feasible to provide remote access to certain users because of insufficient security resources, providing such remote access would not be required.

Comments on rule 2.518. This rule governs remote access by a party's designee. ITAC sought specific comments on an 18-years-of-age cutoff that had been included in the rule as circulated, and sought specific comments on whether designee remote access should be limited to certain case types. The Superior Court of San Joaquin County commented that the age guidelines should match those applied to filings. The Superior Court of San Diego County noted that there should be an exception for emancipated minors and persons over 18 who are under conservatorship. The San Diego court's response, in particular, highlighted to the committee that an age cutoff at 18 was both underinclusive (e.g., excluding emancipated minors) and overinclusive (e.g., including adults under conservatorship). The legal capacity to agree to terms and conditions of a user agreement allowing use of a remote access system is the crux of who may designate. Accordingly, the committee struck the age cutoff from the rule and instead included an advisory committee comment that a party designating must have legal capacity to agree to the terms and conditions of a user agreement.

The Superior Court of Orange County commented that "the rule should be clear that it does not apply to juvenile justice and dependency case types." ITAC agreed because of the sensitivity of the information combined with the fact that counsel are typically involved and attorneys for minors and parents can gain access under other rules. In addition, the Joint Ad Hoc

Subcommittee on Remote Access raised a concern about pressure from gangs to designate gang members to obtain remote access to a person's criminal electronic records. Because of this issue and the sensitivity of the information in these three case types, ITAC agreed and limited the rule so that a party's designee cannot obtain remote access to such records.

The Joint Technology Subcommittee, joined by the Placer court, recommended adding "a statement making clear that the provision of this type of access is optional and not a mandate on the trial courts." ITAC intends the requirements of the rules in article 3 to be tempered by the feasibility condition in rule 2.516. Providing remote access to the users identified in article 3 is only mandatory if it is feasible. If it is not feasible for any reason—for example, lack of sufficient security resources, lack of technical capacity, or lack of financial resources—then it is not mandatory. Finally, the subcommittee recommended adding a rule "that the party must make an affirmative declaration that by granting their designee access to their case file, the trial court and the [j]udicial [b]ranch are absolved of any responsibility or liability for the release of information on their case that is inconsistent with this or other rules or laws." ITAC determined that such a rule is unnecessary because courts can include terms regarding liability in user agreements.

Comments on rule 2.519(c). Subdivision (c) governs remote access by a party's attorney who is not the attorney of record. The Joint Technology Subcommittee, joined by the Placer court, submitted several comments. First, the rule "presents a significant security risk." To address this, ITAC included "security resources" in the advisory committee comments on rule 2.516, which requires courts to provide remote access only if feasible. If providing remote access to attorneys who are not of record is not feasible, then courts are not required to do so. The Joint Technology Subcommittee also commented, "This section appears to contemplate giving access to case information that is otherwise not publicly available, to attorneys who have not formally appeared or associated in as counsel in the case, which might include documents that are not publicly viewable." Rule 2.519, as with the other remote access rules, limits what users can access remotely to the court records they would have been entitled to view at the courthouse. An attorney providing undisclosed representation who showed up at the courthouse would be limited to the same access as the public. Accordingly, the attorney could only remotely access court records that the public could view at the courthouse. The rule merely eliminates the step of the attorney having to go to the courthouse. ITAC added an advisory committee comment to provide clarification about the level of access an undisclosed attorney providing limited scope representation (as opposed to an attorney providing noticed limited scope representation) can gain through remote access.

The Joint Technology Subcommittee also commented that the attorney should be required to provide some kind of noticed representation, but ITAC disagreed. The challenge with limited scope representation in particular is that the attorney may be unknown to the court. Attorneys providing limited scope representation under chapter 3 of title 3 (the civil rules), are permitted to provide noticed representation or undisclosed representation. Requiring an attorney to file a notice of limited scope representation requires notice and service on all parties. (Cal. Rules of

Court, rule 3.36(h).) The requirement to provide noticed representation could add costs to a party who only requires assistance in the drafting of legal documents in his or her matter, or requires assistance with collateral matters. ITAC did not see a clear benefit to requiring noticed representation over the requirements of subdivision (c), which require an attorney who is not of record to "represent [] to the court in the remote access system that the attorney has obtained the party's consent to remotely access the party's electronic records." This provides a mechanism for the court to "know" about the attorney for remote access purposes without requiring a filed notice and service of the notice.

The Joint Technology Subcommittee also commented that there should be "a statement making clear that the provision of this type of access is optional and not a mandate on the trial courts." ITAC intends the requirements of the rules in article 3 to be tempered by the feasibility condition in rule 2.516. Providing remote access to the users identified in article 3 is mandatory only if it is feasible. If it is not feasible for any reason—for example, lack of sufficient security resources, lack of technical capacity, or lack of financial resources—then it is not mandatory.

Comments on rule 2.522. This rule governs remote access by a person working for a qualified legal services project. The Joint Technology Subcommittee, joined by the Placer court, submitted several comments:

- If rule 2.518 (remote access by a party designee) is adopted, rule 5.522 may be unnecessary. ITAC disagreed because although rule 2.518 provides an alternative, it is not sufficient for parties who do not have the ability to gain access to a system to provide designees (e.g., lack computer or Internet access or lack the skills to access). Qualified legal services projects serve indigent populations that may not have access to the resources that would enable them to designate another under rule 2.518.
- If rule 2.519 (remote access by an attorney) is adopted, rule 5.522 again may be unnecessary. ITAC disagreed because rule 2.519 governs attorney remote access only and a person working in a qualified legal organization may not be an attorney (e.g., a paralegal or intern).
- It was unclear how the designation and certification process would work and how records of a party's consent would be documented. ITAC added an advisory committee comment clarifying that the rule does not prescribe particular methods and that courts and qualified legal services projects have flexibility to determine the methods that work for them.
- There may be more technical challenges with implementing rule 2.522 than the other rules. ITAC agreed that it could present a technical challenge, but as with remote access to other users under article 3, the rule is tempered by the feasibility provision of rule 2.516. If it is technically not feasible at the time to provide remote access to users under rule 2.522 then courts would not need to provide remote access to those users.

Comments on rules 2.526 and 2.540. These rules govern audit trails and, as initially proposed, required courts to have the ability to generate audit trails and provide users with the ability to view limited audit trails. The Orange court commented that it was unclear on the purpose of the limited audit trails. ITAC added an advisory committee comment explaining that an audit trail is

meant to be a tool for the court and the users to identify potential issues or misuse of remote access.

In the invitation to comment, ITAC sought specific comments on the challenges of the proposed rule and whether there were more feasible alternatives. The San Joaquin court commented that generating ad hoc reports would be new and require staff, time, and ongoing costs to implement. The court proposed requiring the users to provide good cause before the court would need to provide a report to the user. ITAC agreed that such a provision could reduce the number of reports that would need to be generated, but was unclear what good cause to generate a report would be. ITAC instead followed a suggestion from the Joint Technology Subcommittee, joined by the Placer court, to not make the rule mandatory. The subcommittee commented that "[t]he current mandatory language may result in a court being prohibited from providing any electronic access even with the ability to do so, if the court does not have the ability to provide the required audit trail." A goal of the rules proposal is to facilitate current use of remote access rather than inhibit it. Accordingly, ITAC agreed and recommended making the audit trail rules nonmandatory. However, ITAC recognizes the importance of auditability and added an advisory committee comment that the committee will consider recommending amendments to make the rule mandatory in the future through an invitation to comment.

Comments on rule 2.540. This rule governs remote access by government entities, and subdivision (b) in particular identifies each entity and to what case types authorized users can gain remote access. There is no requirement that the court provide remote access to government entity users even if feasible. Both the Child Support Directors Association of California and the California Department of Child Support Services (CDSS) suggested that the rule be mandatory. ITAC disagreed because the rule was designed to be permissive so the courts can exercise discretion to meet their business needs and capacity. Government entities may still avail themselves of the article 3 rules when they are parties to litigation because their legal staff can gain access under rules 2.519 and 2.520. CDSS also commented that "local child support agency" should be changed to "local child support agencies" so that an agency in one county could potentially remotely access the electronic records of a court situated in another county (rather than a court only dealing with the agency in the county where the court was located). ITAC agreed that a child support agency in one county should not be precluded from obtaining remote access to electronic records of a court in another county. Instead of altering the rule, ITAC added a clarifying advisory committee comment using local child support agencies as an illustrative example. The rules are not written to lock the courts into county boundaries and only allow remote access by government entities in the county where the court is situated and the addition of this advisory committee comment makes that clear.

Alternatives considered

The committee considered making no changes to the rules, but that was not desirable because courts would need to continue providing remote access on a piecemeal, ad hoc basis with no clear authority. Accordingly, ITAC made the creation of these rules a priority on its annual agenda, which was approved by the Judicial Council Technology Committee.

Fiscal and Operational Impacts

Implementation requirements. ITAC solicited specific comments on what the implementation requirements would be on the courts and received the following responses:

- Superior Court of Orange County: "This is dependent upon whether or not courts have existing applications that allow remote access."
- Superior Court of San Diego County:

  [O]ur court has identified the following issues:

  1. Our court needs to understand the business and technical requirements of the implementation. For example, we need to understand the audience that will need access. Will each group of the audience have the same or unique access requirements. For example, do we need to restrict access from specific networks.
  2. Audit and security requirements. Our court needs to be able to generate reports on who, where, when and how long the application was used by remote users.
  3. Testing. Our court needs to be able to identify the testing requirements, especially if the level of access for each audience is different. There needs to be participation from the justice partners (i.e. government agencies).
  4. Training. Tip sheets will need to be prepared for the users.
  5. Legal. There needs to be some kind of MOU with the remote user/justice partner.

- Superior Court of San Joaquin County:

  There will be a level of training necessary to implement a process such as this but it is not possible to specify the exact amount of time necessary to execute all processes. For example, in our court, time and cost must be invested to:

  1. Set up, testing, training, and implementation of an additional program because our current case management system is not set up to handle the identity and audit trails required in the amendment.
  2. Create and train staff assigned to monitor and manage the additional program for questions from the public, account set-up, password management, and any other situation arising from user end regarding remote records access.

Cost savings. ITAC requested specific comments on whether the proposal would provide cost savings and received the following responses:

- Superior Court of Orange County: "No, the administration of managing remote access and unique credentials under these rules will result in ongoing-additional costs. Maintenance of restricted and/or limited term access to remote information will be necessary and require someone to control. Managing user ID's and password control should also be considered."

- Superior Court of San Diego: "No."
- Superior Court of San Joaquin County:

> In the long run there may be some savings due to less walk-in customers at local courthouses[;] however the costs associated to comply with all levels of identity verification and access will create additional ongoing costs for the court. There will also be additional ongoing costs for the addition of staff to monitor, manage, and update all changes required to comply with the identity verification and audit trail requirements. We cannot quantify the savings as we cannot predict the amount of public who will have the means to access court records remotely nor do we know the exact amount of employees needed to maintain these requirements.

Operational impacts. The Joint Technology Subcommittee, joined by the Placer court, noted the following impacts to court operations:

- "The proposal will create the need for new and/or revised procedures and alterations to case management systems. A number of proposed revisions in the proposal would present a workload burden on the trial courts, create new access categories that will result in significant one-time or ongoing costs, and complicate the access rules in a way that may result in confusion for the public."
- "Increases court staff workload—Court staff would be required to verify the identity of individual(s) designated by the party to access their case."
- "Security—The proposed changes could result in security complications and allow for data intrusion."

Attachments and Links

1. Cal. Rules of Court, rules 2.500–2.503, 2.515–2.528, and 2.540–2.545, at pages 17–43
2. Chart of comments, at pages 44-96
3. Link A: Cal. Rules of Court, title 2 (the existing public access rules are rules 2.250–2.261), *http://www.courts.ca.gov/cms/rules/index.cfm?title=two*

Rules 2.500–2.503 of the California Rules of Court are amended and rules 2.515–2.528 and 2.540–2.545 are adopted effective January 1, 2019, to read:

Chapter 2. ~~Public~~ Access to Electronic Trial Court Records

Article 1. General Provisions

Rule 2.500. Statement of purpose

(a) Intent

The rules in this chapter are intended to provide the public, parties, parties' attorneys, legal organizations, court-appointed persons, and government entities with reasonable access to trial court records that are maintained in electronic form, while protecting privacy interests.

(b) Benefits of electronic access

Improved technologies provide courts with many alternatives to the historical paper-based record receipt and retention process, including the creation and use of court records maintained in electronic form. Providing ~~public~~ access to trial court records that are maintained in electronic form may save the courts, ~~and~~ the public, parties, parties' attorneys, legal organizations, court-appointed persons, and government entities time, money, and effort and encourage courts to be more efficient in their operations. Improved access to trial court records may also foster in the public a more comprehensive understanding of the trial court system.

(c) No creation of rights

The rules in this chapter are not intended to give the public, parties, parties' attorneys, legal organizations, court-appointed persons, and government entities a right of access to any record that they are not otherwise legally entitled to access. ~~The rules do not create any right of access to records that are sealed by court order or confidential as a matter of law.~~

Advisory Committee Comment

The rules in this chapter acknowledge the benefits that electronic ~~court~~ records provide but attempt to limit the potential for unjustified intrusions into the privacy of individuals involved in litigation that can occur as a result of remote access to electronic ~~court~~ records. The proposed rules take into account the limited resources currently available in the trial courts. It is contemplated that the rules may be modified to provide greater electronic access as ~~the~~ courts' technical capabilities improve and ~~with the~~ knowledge is gained from the experience of ~~the courts in~~ providing electronic access under these rules.

Rule 2.501. Application, ~~and~~ scope, and information to the public

(a) Application and scope

The rules in this chapter apply only to trial court records as defined in rule 2.502(3). They do not apply to statutorily mandated reporting between or within government entities, or any other documents or materials that are not court records.

(b) ~~Access by parties and attorneys~~ Information to the public

~~The rules in this chapter apply only to access to court records by the public. They do not limit access to court records by a party to an action or proceeding, by the attorney of a party, or by other persons or entities that are entitled to access by statute or rule.~~

The website for each trial court must include a link to information that will inform the public of who may access their electronic records under the rules in this chapter and under what conditions they may do so. This information will be posted publicly on the California Courts website at *www.courts.ca.gov*. Each trial court may post additional information, in plain language, as necessary to inform the public about the level of access that the particular trial court is providing.

Advisory Committee Comment

The rules on remote access do not apply beyond court records to other types of documents, information, or data. Rule 2.502 defines a court record as "any document, paper, or exhibit filed in an action or proceeding; any order or judgment of the court; and any item listed in Government Code section 68151(a)—excluding any reporter's transcript for which the reporter is entitled to receive a fee for any copy—that is maintained by the court in the ordinary course of the judicial process. The term does not include the personal notes or preliminary memoranda of judges or other judicial branch personnel, statutorily mandated reporting between government entities, judicial administrative records, court case information, or compilations of data drawn from court records where the compilations are not themselves contained in a court record." (Cal. Rules of Court, rule 2.502(3).) Thus, courts generate and maintain many types of information that are not court records and to which access may be restricted by law. Such information is not remotely accessible as court records, even to parties and their attorneys. If parties and their attorneys are entitled to access to any such additional information, separate and independent grounds for that access must exist.

Rule 2.502. Definitions

As used in this chapter, the following definitions apply:

(1) "Authorized person" means a person authorized by a legal organization, qualified legal services project, or government entity to access electronic records.

(2) "Brief legal services" means legal assistance provided without, or before, becoming a party's attorney. It includes giving advice, having a consultation, performing research, investigating case facts, drafting documents, and making limited third party contacts on behalf of a client.

~~(1)~~(3) "Court record" is any document, paper, or exhibit filed ~~by the parties to~~ in an action or proceeding; any order or judgment of the court; and any item listed in Government Code section 68151(a)~~,~~ ~~—~~excluding any reporter's transcript for which the reporter is entitled to receive a fee for any copy—that is maintained by the court in the ordinary course of the judicial process. The term does not include the personal notes or preliminary memoranda of judges or other judicial branch personnel, statutorily mandated reporting between or within government entities, judicial administrative records, court case information, or compilations of data drawn from court records where the compilations are not themselves contained in a court record.

(4) "Court case information" refers to data that is stored in a court's case management system or case histories. This data supports the court's management or tracking of the action and is not part of the official court record for the case or cases.

~~(4)~~(5) "Electronic access" means ~~computer~~ access by electronic means to court records available ~~to the public~~ through ~~both~~ public terminals at the courthouse and remotely, unless otherwise specified in the rules in this chapter.

~~(2)~~(6) "Electronic record" is a ~~computerized~~ court record~~, regardless of the manner in which it has been computerized~~ that requires the use of an electronic device to access. The term includes both a ~~document~~ record that has been filed electronically and an electronic copy or version of a record that was filed in paper form. The term does not include a court record that is maintained only on microfiche, paper, or any other medium that can be read without the use of an electronic device.

(7) "Government entity" means a legal entity organized to carry on some function of the State of California or a political subdivision of the State of California. Government entity also means a federally recognized Indian tribe or a reservation, department, subdivision, or court of a federally recognized Indian tribe.

(8) "Legal organization" means a licensed attorney or group of attorneys, nonprofit legal aid organization, government legal office, in-house legal office of a nongovernmental organization, or legal program organized to provide for indigent criminal, civil, or juvenile law representation.

(9) "Party" means a plaintiff, defendant, cross-complainant, cross-defendant, petitioner, respondent, intervenor, objector, or anyone expressly defined by statute as a party in a court case.

(10) "Person" means a natural human being.

~~(3)~~(11) "The public" means ~~an individual~~ a person, a group, or an entity, including print or electronic media, ~~or the representative of an individual, a group, or an entity~~ regardless of any legal or other interest in a particular court record.

(12) "Qualified legal services project" has the same meaning under the rules of this chapter as in Business and Professions Code section 6213(a).

(13) "Remote access" means electronic access from a location other than a public terminal at the courthouse.

(14) "User" means an individual person, a group, or an entity that accesses electronic records.

Article 2. Public Access

Rule 2.503. ~~Public access~~ Application and scope

(a) General right of access by the public

(1) All electronic records must be made reasonably available to the public in some form, whether in electronic or in paper form, except those that are sealed by court order or made confidential by law.

(2) The rules in this article apply only to access to electronic records by the public.

(b) Electronic access required to extent feasible

A court that maintains the following records in electronic form must provide electronic access to them, both remotely and at the courthouse, to the extent it is feasible to do so:

(1) Registers of actions (as defined in Gov. Code, § 69845), calendars, and indexes in all cases; and

(2) All court records in civil cases, except those listed in (c)(1)–~~(9)~~(11).

(c) Courthouse electronic access only

A court that maintains the following records in electronic form must provide electronic access to them at the courthouse, to the extent it is feasible to do so, but may not provide public remote ~~electronic~~ access to these records ~~only to the records governed by (b)~~:

(1) Records in a proceeding under the Family Code, including proceedings for dissolution, legal separation, and nullity of marriage; child and spousal support proceedings; child custody proceedings; and domestic violence prevention proceedings;

(2) Records in a juvenile court proceeding;

(3) Records in a guardianship or conservatorship proceeding;

(4) Records in a mental health proceeding;

(5) Records in a criminal proceeding;

(6) Records in proceedings to compromise the claims of a minor or a person with a disability;

(7)~~(6)~~ Records in a civil harassment proceeding under Code of Civil Procedure section 527.6;

(8)~~(7)~~ Records in a workplace violence prevention proceeding under Code of Civil Procedure section 527.8;

(9)~~(8)~~ Records in a private postsecondary school violence prevention proceeding under Code of Civil Procedure section 527.85;

(10)~~(9)~~ Records in an elder or dependent adult abuse prevention proceeding under Welfare and Institutions Code section 15657.03; and

~~(10) Records in proceedings to compromise the claims of a minor or a person with a disability.~~

(11) Records in a gun violence prevention proceeding under Penal Code sections 18100–18205.

(d) * * *

(e) Remote ~~electronic~~ access allowed in extraordinary criminal cases

Notwithstanding (c)(5), the presiding judge of the court, or a judge assigned by the presiding judge, may exercise discretion, subject to (e)(1), to permit remote ~~electronic~~ access by the public to all or a portion of the public court records in an individual criminal case if (1) the number of requests for access to documents in the case is extraordinarily high and (2) responding to those requests would significantly burden the operations of the court. An individualized determination must be made in each case in which such remote ~~electronic~~ access is provided.

(1) In exercising discretion under (e), the judge should consider the relevant factors, such as:

(A) * * *

(B) The benefits to and burdens on the parties in allowing remote ~~electronic~~ access, including possible impacts on jury selection; and

(C) * * *

(2) The court should, to the extent feasible, redact the following information from records to which it allows remote access under (e): driver license numbers; dates of birth; social security numbers; Criminal Identification and Information and National Crime Information numbers; addresses and phone numbers of parties, victims, witnesses, and court personnel; medical or psychiatric information; financial information; account numbers; and other personal identifying information. The court may order any party who files a document containing such information to provide the court with both an original unredacted version of the document for filing in the court file and a redacted version of the document for remote ~~electronic~~ access. No juror names or other juror identifying information may be provided by remote ~~electronic~~ access. This subdivision does not apply to any document in the original court file; it applies only to documents that are available by remote ~~electronic~~ access.

(3) Five days' notice must be provided to the parties and the public before the court makes a determination to provide remote ~~electronic~~ access under this

rule. Notice to the public may be accomplished by posting notice on the court's ~~Web site~~ website. Any person may file comments with the court for consideration, but no hearing is required.

(4) The court's order permitting remote ~~electronic~~ access must specify which court records will be available by remote ~~electronic~~ access and what categories of information are to be redacted. The court is not required to make findings of fact. The court's order must be posted on the court's ~~Web site~~ website and a copy sent to the Judicial Council.

(f)–(i) *** * ***

Advisory Committee Comment

The rule allows a level of access by the public to all electronic records that is at least equivalent to the access that is available for paper records and, for some types of records, is much greater. At the same time, it seeks to protect legitimate privacy concerns.

Subdivision (c). This subdivision excludes certain records (those other than the register, calendar, and indexes) in specified types of cases (notably criminal, juvenile, and family court matters) from public remote ~~electronic~~ access. The committee recognized that while these case records are public records and should remain available at the courthouse, either in paper or electronic form, they often contain sensitive personal information. The court should not publish that information over the Internet. However, the committee also recognized that the use of the Internet may be appropriate in certain criminal cases of extraordinary public interest where information regarding a case will be widely disseminated through the media. In such cases, posting of selected nonconfidential court records, redacted where necessary to protect the privacy of the participants, may provide more timely and accurate information regarding the court proceedings, and may relieve substantial burdens on court staff in responding to individual requests for documents and information. Thus, under subdivision (e), if the presiding judge makes individualized determinations in a specific case, certain records in criminal cases may be made available over the Internet.

Subdivisions (f) and (g). These subdivisions limit electronic access to records (other than the register, calendars, or indexes) to a case-by-case basis and prohibit bulk distribution of those records. These limitations are based on the qualitative difference between obtaining information from a specific case file and obtaining bulk information that may be manipulated to compile personal information culled from any document, paper, or exhibit filed in a lawsuit. This type of aggregate information may be exploited for commercial or other purposes unrelated to the operations of the courts, at the expense of privacy rights of individuals.

Courts must send a copy of the order permitting remote ~~electronic~~ access in extraordinary criminal cases to~~:~~ Criminal Justice Services, Judicial Council of California, 455 Golden Gate Avenue, San Francisco, CA 94102-3688.

Rules 2.504–2.507 * * *

Article 3. Remote Access by a Party, Party's Designee, Party's Attorney, Court-Appointed Person, or Authorized Person Working in a Legal Organization or Qualified Legal Services Project

Rule 2.515. Application and scope

(a) No limitation on access to electronic records available under article 2

The rules in this article do not limit remote access to electronic records available under article 2. These rules govern access to electronic records where remote access by the public is not allowed.

(b) Who may access

The rules in this article apply to remote access to electronic records by:

(1) A person who is a party;

(2) A designee of a person who is a party;

(3) A party's attorney;

(4) An authorized person working in the same legal organization as a party's attorney;

(5) An authorized person working in a qualified legal services project providing brief legal services; and

(6) A court-appointed person.

Advisory Committee Comment

Article 2 allows remote access in most civil cases, and the rules in article 3 are not intended to limit that access. Rather, the article 3 rules allow broader remote access—by parties, parties' designees, parties' attorneys, authorized persons working in legal organizations, authorized

persons working in a qualified legal services project providing brief services, and court-appointed persons—to those electronic records where remote access by the public is not allowed.

Under the rules in article 3, a party, a party's attorney, an authorized person working in the same legal organization as a party's attorney, or a person appointed by the court in the proceeding basically has the same level of access to electronic records remotely that he or she would have if he or she were to seek to inspect the records in person at the courthouse. Thus, if he or she is legally entitled to inspect certain records at the courthouse, that person could view the same records remotely; on the other hand, if he or she is restricted from inspecting certain court records at the courthouse (e.g., because the records are confidential or sealed), that person would not be permitted to view the records remotely. In some types of cases, such as unlimited civil cases, the access available to parties and their attorneys is generally similar to the public's but in other types of cases, such as juvenile cases, it is much more extensive (see Cal. Rules of Court, rule 5.552).

For authorized persons working in a qualified legal services program, the rule contemplates services offered in high-volume environments on an ad hoc basis. There are some limitations on access under the rule for qualified legal services projects. When an attorney at a qualified legal services project becomes a party's attorney and offers services beyond the scope contemplated under this rule, the access rules for a party's attorney would apply.

Rule 2.516. Remote access to extent feasible

To the extent feasible, a court that maintains records in electronic form must provide remote access to those records to the users described in rule 2.515, subject to the conditions and limitations stated in this article and otherwise provided by law.

Advisory Committee Comment

This rule takes into account the limited resources currently available in some trial courts. Many courts may not have the financial means, security resources, or technical capabilities necessary to provide the full range of remote access to electronic records authorized by this article. When it is more feasible and courts have had more experience with remote access, these rules may be amended to further expand remote access.

This rule is not intended to prevent a court from moving forward with the limited remote access options outlined in this rule as such access becomes feasible. For example, if it were only feasible for a court to provide remote access to parties who are persons, it could proceed to provide remote access to those users only.

Rule 2.517. Remote access by a party

(a) Remote access generally permitted

A person may have remote access to electronic records in actions or proceedings in which that person is a party.

(b) Level of remote access

(1) In any action or proceeding, a party may be provided remote access to the same electronic records that he or she would be legally entitled to inspect at the courthouse.

(2) This rule does not limit remote access to electronic records available under article 2.

(3) This rule applies only to electronic records. A person is not entitled under these rules to remote access to documents, information, data, or other materials created or maintained by the courts that are not electronic records.

Advisory Committee Comment

Because this rule permits remote access only by a party who is a person (defined under rule 2.501 as a natural human being), remote access would not apply to parties that are organizations, which would need to gain remote access under the party's attorney rule or, for certain government entities with respect to specified electronic records, the rules in article 4.

A party who is a person would need to have the legal capacity to agree to the terms and conditions of a court's remote access user agreement before using a system of remote access. The court could deny access or require additional information if the court knew the person seeking access lacked legal capacity or appeared to lack capacity—for example, if identity verification revealed the person seeking access was a minor.

Rule 2.518. Remote access by a party's designee

(a) Remote access generally permitted

A person who is a party in an action or proceeding may designate other persons to have remote access to electronic records in that action or proceeding.

(b) Level of remote access

(1) Except for criminal electronic records, juvenile justice electronic records, and child welfare electronic records, a party's designee may have the same access to a party's electronic records that a member of the public would be entitled to if he or she were to inspect the party's court records at the courthouse. A party's designee is not permitted remote access to criminal electronic records, juvenile justice electronic records, and child welfare electronic records.

(2) A party may limit the access to be afforded a designee to specific cases.

(3) A party may limit the access to be afforded a designee to a specific period of time.

(4) A party may modify or revoke a designee's level of access at any time.

(c) Terms of access

(1) A party's designee may access electronic records only for the purpose of assisting the party or the party's attorney in the action or proceeding.

(2) Any distribution for sale of electronic records obtained remotely under the rules in this article is strictly prohibited.

(3) All laws governing confidentiality and disclosure of court records apply to the records obtained under this article.

(4) Party designees must comply with any other terms of remote access required by the court.

(5) Failure to comply with these rules may result in the imposition of sanctions, including termination of access.

Advisory Committee Comment

A party must be a natural human being with the legal capacity to agree to the terms and conditions of a user agreement with the court to authorize designees for remote access. Under rule 2.501, for purposes of the rules, "person" refers to natural human beings Accordingly, the party's designee rule would not apply to parties that are organizations, which would need to gain remote access under the party's attorney rule or, for certain government entities with respect to specified electronic records, under the rules in article 4.

Rule 2.519. Remote access by a party's attorney

(a) Remote access generally permitted

(1) A party's attorney may have remote access to electronic records in the party's actions or proceedings under this rule or under rule 2.518. If a party's attorney gains remote access under rule 2.518, the requirements of rule 2.519 do not apply.

(2) If a court notifies an attorney of the court's intention to appoint the attorney to represent a party in a criminal, juvenile justice, child welfare, family law, or probate proceeding, the court may grant remote access to that attorney before an order of appointment is issued by the court.

(b) Level of remote access

A party's attorney may be provided remote access to the same electronic records in the party's actions or proceedings that the party's attorney would be legally entitled to view at the courthouse.

(c) Terms of remote access applicable to an attorney who is not the attorney of record

An attorney who represents a party, but who is not the party's attorney of record in the party's actions or proceedings, may remotely access the party's electronic records, provided that the attorney:

(1) Obtains the party's consent to remotely access the party's electronic records; and

(2) Represents to the court in the remote access system that he or she has obtained the party's consent to remotely access the party's electronic records.

(d) Terms of remote access applicable to all attorneys

(1) A party's attorney may remotely access the electronic records only for the purpose of assisting the party with the party's court matter.

(2) A party's attorney may not distribute for sale any electronic records obtained remotely under the rules in this article. Such sale is strictly prohibited.

(3) A party's attorney must comply with any other terms of remote access required by the court.

(4) Failure to comply with these rules may result in the imposition of sanctions, including termination of access.

Advisory Committee Comment

Subdivision (c). An attorney of record will be known to the court for purposes of remote access. However, a person may engage an attorney other than the attorney of record for assistance in an action or proceeding in which the person is a party. For example, a party may engage an attorney to (1) prepare legal documents but not appear in the party's action (e.g., provide limited-scope representation); (2) assist the party with dismissal or sealing of a criminal record when the attorney did not represent the party in the criminal proceeding; or (3) represent the party in an appellate matter when the attorney did not represent the party in the trial court. Subdivision (c) provides a mechanism for an attorney not of record to be known to the court for purposes of remote access.

Because the level of remote access is limited to the same court records that an attorney would be entitled to access if he or she were to appear at the courthouse, an attorney providing undisclosed representation would only be able to remotely access electronic records that the public could access at the courthouse. The rule essentially removes the step of the attorney having to go to the courthouse.

Rule 2.520. Remote access by persons working in the same legal organization as a party's attorney

(a) Application and scope

(1) This rule applies when a party's attorney is assisted by others working in the same legal organization.

(2) "Working in the same legal organization" under this rule includes partners, associates, employees, volunteers, and contractors.

(3) This rule does not apply when a person working in the same legal organization as a party's attorney gains remote access to records as a party's designee under rule 2.518.

(b) Designation and certification

(1) A party's attorney may designate that other persons working in the same legal organization as the party's attorney have remote access.

(2) A party's attorney must certify that the other persons authorized for remote access are working in the same legal organization as the party's attorney and are assisting the party's attorney in the action or proceeding.

(c) Level of remote access

(1) Persons designated by a party's attorney under (b) must be provided access to the same electronic records as the party.

(2) Notwithstanding (b), when a court designates a legal organization to represent parties in criminal, juvenile, family, or probate proceedings, the court may grant remote access to a person working in the organization who assigns cases to attorneys working in that legal organization.

(d) Terms of remote access

(1) Persons working in a legal organization may remotely access electronic records only for purposes of assigning or assisting a party's attorney.

(2) Any distribution for sale of electronic records obtained remotely under the rules in this article is strictly prohibited.

(3) All laws governing confidentiality and disclosure of court records apply to the records obtained under this article.

(4) Persons working in a legal organization must comply with any other terms of remote access required by the court.

(5) Failure to comply with these rules may result in the imposition of sanctions, including termination of access.

Advisory Committee Comment

Subdivision (b). The designation and certification outlined in this subdivision need only be done once and can be done at the time the attorney establishes his or her remote access account with the court.

Rule 2.521. Remote access by a court-appointed person

(a) Remote access generally permitted

(1) A court may grant a court-appointed person remote access to electronic records in any action or proceeding in which the person has been appointed by the court.

(2) Court-appointed persons include an attorney appointed to represent a minor child under Family Code section 3150; a Court Appointed Special Advocate volunteer in a juvenile proceeding; an attorney appointed under Probate Code section 1470, 1471, or 1474; an investigator appointed under Probate Code section 1454; a probate referee designated under Probate Code section 8920; a fiduciary, as defined in Probate Code section 39; an attorney appointed under Welfare and Institutions Code section 5365; or a guardian ad litem appointed under Code of Civil Procedure section 372 or Probate Code section 1003.

(b) Level of remote access

A court-appointed person may be provided with the same level of remote access to electronic records as the court-appointed person would be legally entitled to if he or she were to appear at the courthouse to inspect the court records.

(c) Terms of remote access

(1) A court-appointed person may remotely access electronic records only for purposes of fulfilling the responsibilities for which he or she was appointed.

(2) Any distribution for sale of electronic records obtained remotely under the rules in this article is strictly prohibited.

(3) All laws governing confidentiality and disclosure of court records apply to the records obtained under this article.

(4) A court-appointed person must comply with any other terms of remote access required by the court.

(5) Failure to comply with these rules may result in the imposition of sanctions, including termination of access.

Rule 2.522. Remote access by persons working in a qualified legal services project providing brief legal services

(a) Application and scope

(1) This rule applies to qualified legal services projects as defined in Business and Professions Code section 6213(a).

(2) "Working in a qualified legal services project" under this rule includes attorneys, employees, and volunteers.

(3) This rule does not apply to a person working in or otherwise associated with a qualified legal services project who gains remote access to court records as a party's designee under rule 2.518.

(b) Designation and certification

(1) A qualified legal services project may designate persons working in the qualified legal services project who provide brief legal services, as defined in rule 2.501, to have remote access.

(2) The qualified legal services project must certify that the authorized persons work in their organization.

(c) Level of remote access

Authorized persons may be provided remote access to the same electronic records that the authorized person would be legally entitled to inspect at the courthouse.

(d) Terms of remote access

(1) Qualified legal services projects must obtain the party's consent to remotely access the party's electronic records.

(2) Authorized persons must represent to the court in the remote access system that the qualified legal services project has obtained the party's consent to remotely access the party's electronic records.

(3) Qualified legal services projects providing services under this rule may remotely access electronic records only to provide brief legal services.

(4) Any distribution for sale of electronic records obtained under the rules in this article is strictly prohibited.

(5) All laws governing confidentiality and disclosure of court records apply to electronic records obtained under this article.

(6) Qualified legal services projects must comply with any other terms of remote access required by the court.

(7) Failure to comply with these rules may result in the imposition of sanctions, including termination of access.

Advisory Committee Comment

The rule does not prescribe any particular method for capturing the designation and certification of persons working in a qualified legal services project. Courts and qualified legal services projects have flexibility to determine what method would work for both entities. For example, the information could be captured in a remote access system if an organizational-level account could be established, or the information could be captured in a written agreement between the court and the qualified legal services project.

The rule does not prescribe any particular method for a qualified legal services project to document the consent it obtained to access a person's electronic records. Qualified legal services projects have flexibility to adapt the requirement to their regular processes for making records. For example, the qualified legal services project could obtain a signed consent form for its records or could obtain consent over the phone and make an entry to that effect in its records, or the court and the qualified legal services project could enter into an agreement to describe how consent will be obtained and recorded.

Rule 2.523. Identity verification, identity management, and user access

(a) Identity verification required

Except for remote access provided to a party's designee under rule 2.518, before allowing a person who is eligible under the rules in article 3 to have remote access to electronic records, a court must verify the identity of the person seeking access.

(b) Responsibilities of the court

A court that allows persons eligible under the rules in article 3 to have remote access to electronic records must have an identity verification method that verifies the identity of, and provides a unique credential to, each person who is permitted remote access to the electronic records. The court may authorize remote access by a person only if that person's identity has been verified, the person accesses records

using the credential provided to that individual, and the person complies with the terms and conditions of access, as prescribed by the court.

(c) Responsibilities of persons accessing records

A person eligible to be given remote access to electronic records under the rules in article 3 may be given such access only if that person:

(1) Provides the court with all information it directs in order to identify the person to be a user;

(2) Consents to all conditions for remote access required under article 3 and by the court; and

(3) Is authorized by the court to have remote access to electronic records.

(d) Responsibilities of the legal organizations or qualified legal services projects

(1) If a person is accessing electronic records on behalf of a legal organization or qualified legal services project, the organization or project must approve granting access to that person, verify the person's identity, and provide the court with all the information it directs in order to authorize that person to have access to electronic records.

(2) If a person accessing electronic records on behalf of a legal organization or qualified legal services project leaves his or her position or for any other reason is no longer entitled to access, the organization or project must immediately notify the court so that it can terminate the person's access.

(e) Vendor contracts, statewide master agreements, and identity and access management systems

A court may enter into a contract with a vendor to provide identity verification, identity management, or user access services. Alternatively, courts may use a statewide identity verification, identity management, or access management system, if available, or a statewide master agreement for such systems, if available.

Advisory Committee Comment

Subdivisions (a) and (d). A court may verify user identities under (a) by obtaining a representation from a legal organization or qualified legal services project that the legal organization or qualified legal services project has verified the user identities under (d). No additional verification steps are required on the part of the court.

Rule 2.524. Security of confidential information

(a) Secure access and encryption required

If any information in an electronic record that is confidential by law or sealed by court order may lawfully be provided remotely to a person or organization described in rule 2.515, any remote access to the confidential information must be provided through a secure platform and any electronic transmission of the information must be encrypted.

(b) Vendor contracts and statewide master agreements

A court may enter into a contract with a vendor to provide secure access and encryption services. Alternatively, if a statewide master agreement is available for secure access and encryption services, courts may use that master agreement.

Advisory Committee Comment

This rule describes security and encryption requirements; levels of access are provided for in rules 2.517–2.522.

Rule 2.525. Searches; unauthorized access

(a) Searches by case number or caption

A user authorized under this article to remotely access a party's electronic records may search for the records by case number or case caption.

(b) Access level

A court providing remote access to electronic records under this article must ensure that authorized users are able to access the electronic records only at the access levels provided in this article.

(c) Unauthorized access

If a user gains access to an electronic record that he or she is not authorized to access under this article, the user must:

(1) Report the unauthorized access to the court as directed by the court for that purpose;

(2) Destroy all copies, in any form, of the record; and

(3) Delete from his or her web browser history all information that identifies the record.

Rule 2.526. Audit trails

(a) Ability to generate audit trails

The court should have the ability to generate an audit trail that contains one or more of the following elements: what electronic record was remotely accessed, when it was remotely accessed, who remotely accessed it, and under whose authority the user gained access.

(b) Limited audit trails available to authorized users

(1) A court providing remote access to electronic records under this article should make limited audit trails available to authorized users under this article.

(2) A limited audit trail should identify the user who remotely accessed electronic records in a particular case, but must not identify which specific electronic records were accessed.

Advisory Committee Comment

The audit trail is a tool to assist the courts and users in identifying and investigating any potential issues or misuse of remote access. The user's view of the audit trail is limited to protect sensitive information.

To facilitate the use of existing remote access systems, rule 2.526 is currently not mandatory, but may be amended to be mandatory in the future.

Rule 2.527. Additional conditions of access

To the extent consistent with these rules and other applicable law, a court must impose reasonable conditions on remote access to preserve the integrity of its records, prevent the unauthorized use of information, and limit possible legal liability. The court may choose

to require each user to submit a signed, written agreement enumerating those conditions before it permits that user to remotely access electronic records. The agreements may define the terms of access, provide for compliance audits, specify the scope of liability, and provide for sanctions for misuse up to and including termination of remote access.

Rule 2.528. Termination of remote access

(a) Remote access is a privilege

Remote access to electronic records under this article is a privilege and not a right.

(b) Termination by court

A court that provides remote access may, at any time and for any reason, terminate the permission granted to any person eligible under the rules in article 3 to remotely access electronic records.

Article 4. Remote Access by Government Entities

Rule 2.540. Application and scope

(a) Applicability to government entities

The rules in this article provide for remote access to electronic records by government entities described in (b). The access allowed under these rules is in addition to any access these entities or authorized persons working for such entities may have under the rules in articles 2 and 3.

(b) Level of remote access

(1) A court may provide authorized persons from government entities with remote access to electronic records as follows:

(A) Office of the Attorney General: criminal electronic records and juvenile justice electronic records.

(B) California Department of Child Support Services: family electronic records, child welfare electronic records, and parentage electronic records.

(C) Office of a district attorney: criminal electronic records and juvenile justice electronic records.

(D) Office of a public defender: criminal electronic records and juvenile justice electronic records.

(E) Office of a county counsel: criminal electronic records, mental health electronic records, child welfare electronic records, and probate electronic records.

(F) Office of a city attorney: criminal electronic records, juvenile justice electronic records, and child welfare electronic records.

(G) County department of probation: criminal electronic records, juvenile justice electronic records, and child welfare electronic records.

(H) County sheriff's department: criminal electronic records and juvenile justice electronic records.

(I) Local police department: criminal electronic records and juvenile justice electronic records.

(J) Local child support agency: family electronic records, child welfare electronic records, and parentage electronic records.

(K) County child welfare agency: child welfare electronic records.

(L) County public guardian: criminal electronic records, mental health electronic records, and probate electronic records.

(M) County agency designated by the board of supervisors to provide conservatorship investigation under chapter 3 of the Lanterman-Petris-Short Act (Welf. & Inst. Code, §§ 5350–5372): criminal electronic records, mental health electronic records, and probate electronic records.

(N) Federally recognized Indian tribe (including any reservation, department, subdivision, or court of the tribe) with concurrent jurisdiction: child welfare electronic records, family electronic records, juvenile justice electronic records, and probate electronic records.

(O) For good cause, a court may grant remote access to electronic records in particular case types to government entities beyond those listed in

(b)(1)(A)–(N). For purposes of this rule, "good cause" means that the government entity requires access to the electronic records in order to adequately perform its statutory duties or fulfill its responsibilities in litigation.

(P) All other remote access for government entities is governed by articles 2 and 3.

(2) Subject to (b)(1), the court may provide a government entity with the same level of remote access to electronic records as the government entity would be legally entitled to if a person working for the government entity were to appear at the courthouse to inspect court records in that case type. If a court record is confidential by law or sealed by court order and a person working for the government entity would not be legally entitled to inspect the court record at the courthouse, the court may not provide the government entity with remote access to the confidential or sealed electronic record.

(3) This rule applies only to electronic records. A government entity is not entitled under these rules to remote access to any documents, information, data, or other types of materials created or maintained by the courts that are not electronic records.

(c) Terms of remote access

(1) Government entities may remotely access electronic records only to perform official duties and for legitimate governmental purposes.

(2) Any distribution for sale of electronic records obtained remotely under the rules in this article is strictly prohibited.

(3) All laws governing confidentiality and disclosure of court records apply to electronic records obtained under this article.

(4) Government entities must comply with any other terms of remote access required by the court.

(5) Failure to comply with these requirements may result in the imposition of sanctions, including termination of access.

Advisory Committee Comment

The rule does not restrict courts to providing remote access only to local government entities in the same county in which the court is situated. For example, a court in one county could allow remote access to electronic records by a local child support agency in a different county.

Subdivision (b)(3). As to the applicability of the rules on remote access only to electronic records, see the advisory committee comment to rule 2.501.

Rule 2.541. Identity verification, identity management, and user access

(a) Identity verification required

Before allowing a person or entity eligible under the rules in article 4 to have remote access to electronic records, a court must verify the identity of the person seeking access.

(b) Responsibilities of the courts

A court that allows persons eligible under the rules in article 4 to have remote access to electronic records must have an identity verification method that verifies the identity of, and provides a unique credential to, each person who is permitted remote access to the electronic records. The court may authorize remote access by a person only if that person's identity has been verified, the person accesses records using the name and password provided to that individual, and the person complies with the terms and conditions of access, as prescribed by the court.

(c) Responsibilities of persons accessing records

A person eligible to remotely access electronic records under the rules in article 4 may be given such access only if that person:

(1) Provides the court with all of the information it needs to identify the person to be a user;

(2) Consents to all conditions for remote access required by article 4 and the court; and

(3) Is authorized by the court to have remote access to electronic records.

(d) Responsibilities of government entities

(1) If a person is accessing electronic records on behalf of a government entity, the government entity must approve granting access to that person, verify the person's identity, and provide the court with all the information it needs to authorize that person to have access to electronic records.

(2) If a person accessing electronic records on behalf of a government entity leaves his or her position or for any other reason is no longer entitled to access, the government entity must immediately notify the court so that the court can terminate the person's access.

(e) Vendor contracts, statewide master agreements, and identity and access management systems

A court may enter into a contract with a vendor to provide identity verification, identity management, or user access services. Alternatively, courts may use a statewide identity verification, identity management, or access management system, if available, or a statewide master agreement for such systems, if available.

Rule 2.542. Security of confidential information

(a) Secure access and encryption required

If any information in an electronic record that is confidential by law or sealed by court order may lawfully be provided remotely to a government entity, any remote access to the confidential information must be provided through a secure platform, and any electronic transmission of the information must be encrypted.

(b) Vendor contracts and statewide master agreements

A court may enter into a contract with a vendor to provide secure access and encryption services. Alternatively, if a statewide master agreement is available for secure access and encryption services, courts may use that master agreement.

Rule 2.543. Audit trails

(a) Ability to generate audit trails

The court should have the ability to generate an audit trail that contains one or more of the following elements: what electronic record was remotely accessed, when it was accessed, who accessed it, and under whose authority the user gained access.

(b) Audit trails available to government entity

(1) A court providing remote access to electronic records under this article should make limited audit trails available to authorized users of the government entity.

(2) A limited audit trail should identify the user who remotely accessed electronic records in a particular case, but must not identify which specific electronic records were accessed.

Advisory Committee Comment

The audit trail is a tool to assist the courts and users in identifying and investigating any potential issues or misuse of remote access. The user's view of the audit trail is limited to protect sensitive information.

To facilitate the use of existing remote access systems, rule 2.526 is currently not mandatory, but may be amended to be mandatory in the future.

Rule 2.544. Additional conditions of access

To the extent consistent with these rules and other applicable law, a court must impose reasonable conditions on remote access to preserve the integrity of its records, prevent the unauthorized use of information, and limit possible legal liability. The court may choose to require each user to submit a signed, written agreement enumerating those conditions before it permits that user to access electronic records remotely. The agreements may define the terms of access, provide for compliance audits, specify the scope of liability, and provide for sanctions for misuse up to and including termination of remote access.

Rule 2.545. Termination of remote access

(a) Remote access is a privilege

Remote access to electronic records under this article is a privilege and not a right.

(b) Termination by court

A court that provides remote access may, at any time and for any reason, terminate the permission granted to any person or entity eligible under the rules in article 4 to remotely access electronic records

ITC SPR18-37
Technology: Remote Access to Electronic Records

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
1	California Child Support Directors Association By Greg Wilson, MPPA, CAE Executive Director 2150 River Plaza Drive, Suite 420 Sacramento, CA 95833 Tel: 916-446-6700 Fax: 916-446-1199 www.csdaca.org	AM	Thank you for this opportunity to provide formal Comment to Judicial Council proposal SPR18-37, titled "Technology: Remote Access to Electronic Records". This letter is written on behalf of the California Child Support Directors Association (CSDA). The CSDA was established in 2000 as a non-profit association to represent the local child support directors of California's 58 counties. The CSDA strives to be of service to local child support agencies (LCSAs) in their efforts to provide children and families with the financial, medical, and emotional support required to be productive and healthy citizens in our society. California's Child Support Program collects over $2-4 billion annually for the one million children it serves. LCSAs and their staff work directly with the Courts to accomplish the core purpose of establishing parentage, and establishing and enforcing support orders, as set forth in Family Code§ 17400.	The committee appreciates the comments, but declines to modify the proposed rule to make it mandatory for the court rather than permissive. The access by government entities in article 4 is meant to be permissive on the part of the court. The rules only govern remote access and not access in general to the courts. Courthouse access should still be an option. While a statewide level of remote access to all 58 courts' electronic records may be desirable, the courts should be able to exercise discretion in this area to meet their business needs and capacity.

Positions: A = Agree; AM = Agree if modified; N = Do not agree; NI = Not indicated

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			The purpose of this letter is to comment on a specific section of SPR18-37, regarding the following section at pp. 30-31 of the proposal: Article 4. Remote Access by Government Entities, Rule 2.54o(b), which provides: **(b) Level of remote access** (1) A court may provide authorized persons from government entities with remote access to electronic records as follows: . . . (B) California Department of Child Support Services: family electronic records, child welfare electronic records, and parentage electronic records. [Emphasis added] This proposed Rule of Court is a positive development, in that it moves in the direction of promoting efficiency in the Child Support Program by proposing a	

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			court rule as legal authorization to the court and judicial officers the discretion to give LCSAs access to court records regarding parentage in Uniform Parentage Act cases. However, the CSDA suggests the following language as to subsection (b)(1): (1) A court shall provide authorized persons from government entities with remote access to electronic records as follows: By changing "may" to "shall", at least in the context of LCSA access to court records within the scope of this comment, LCSAs throughout the state will be assured of consistent application of the Rule of Court by each Court within the State of California. This in turn will ensure that each LCSA throughout the State will enjoy the same level of access to the	

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			electronic records specified in subdivision (b)(1)(B). Conversely, the use of "may" as proposed, will allow individual courts to determine, in their discretion, whether to allow access to the records or not. We fear that approval of the Rule of Court in its present draft form, essentially providing discretion to allow access to the records, will lead to inconsistent results between Courts, and therefore, inconsistent access and levels of customer services to the LCSAs, and therefore, to the customers, families and children whom the child support program is mandated to serve. Moreover, amending the proposed Rule of Court to be directory, using "shall" will save Court time and resource in having to determine on a case-by-case basis, whether to exercise discretion in allowing access to the records. There may	

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			be increased motion activity and use of court time to resolve access issues on a case-by-case basis should the discretionary language of "may" not be amended to a uniform standard using "shall". The CSDA appreciates the Judicial Council's consideration of this comment and appreciates the opportunity to provide input in this process.	
2	California Department of Child Support Services By Kristen Donadee, Assistant Chief Counsel; Leslie Carmona, Attorney III Office of Legal Services Tel: 916-464-5181 Fax: 916-464-5069 Leslie.Carmona@dcss.ca.gov	AM	The California Department of Child Support Services (Department) has reviewed the proposal identified above for potential impacts to the child support program, the local child support agencies (LCSAs), and our case participants. Specific feedback related to the provisions of the rule with potential impacts to the Department and its Stakeholders follows. Rule 2.540	The committee appreciates the comments. The committee declines to make rule 2.540 mandatory. It is permissive so the courts can exercise discretion to meet their business needs and capacity. The proposal is intended to provide statewide authority, structure, and guidance to the courts. Though statewide uniformity in the child support program may be a desirable outcome, it is not the goal of the proposal.

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			The Department supports the adoption of this rule for the following reasons: 1) It clarifies that the Judicial Council of California (JCC) has determined that providing justice partners with remote access is a public policy it supports; 2) It encourages trial courts to provide remote access to the extent supported by their court case management system; 3) It recognizes that such access would reduce impacts on court clerks; and 4) It best serves the needs of individuals receiving services from government entities. The Department recognizes that the JCC cannot impose a requirement that all courts provide remote access to their high-volume justice partners at this time due to the lack of a single statewide court case management system. However,	The committee declines to combine Department of Child Support Services with local child support agencies. The rules were intentionally organized by each individual government entity. It is possible that government entities under rule 2.240(b) may be treated differently in terms of remote access, but it is in the court's discretion to provide remote access to government entities. The court is in the best position to know its business needs and capacity to provide remote access to each type of government entity. In addition, incorporating them in the same rule could be read as requiring the courts to take an "all or none" approach with these entities and the subcommittee does not believe that is a desirable outcome. The committee declines to make "local child support agency" plural in rule 2.540(b)(1)(B), but will instead address the issue in advisory committee comments because this could apply not only to local child

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			there is an opportunity for the JCC to promote greater court access for high volume justice partners than is contemplated by the permissive rule as drafted. More specifically, the Department would encourage the JCC to consider amending the rule to mandate that trial courts provide remote access to local court case management systems when feasible. The Department also appreciates formal recognition by the JCC that remote access to multiple case types supports the ability of the child support program, as a whole, to discharge its state and local mandates effectively. Such access helps the Department provide vitial [sic] information about all court orders entered in California to the Federal Parent Locator System. Remote access is also valuable because it permits local child support agencies to have timely access to information about any onoing in-state court	support agencies, but other local government entities as well. While the rules are not written to lock the courts into the county boundaries and only allow remote access by government entities in the county where the court resides, an advisory committee comment should make this clear. The committee declines to include non-exhaustive list of authorities on "parentage" as it is unnecessary. Finally, the committee declines to add language about fees. Fees are outside the scope of the rules proposal. To the extent there may be shared funding or costs between the courts and government entities, those matters can be handled through the agreements between the courts and the government entities.

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			proceedings and the existence of California parentage and child support judgments. Access to this vital case information helps ensure that local child support agencies do not ask courts to enter conflicting or void child support judgments.· That said, the Department has concerns that the rule, as drafted, may not achieve statewide uniformity for the child support program as the JCC appears to intend. To amerilorate this risk, the Department respectfully requests that the JCC consider amending the child support provisions of Rule 2.540(b)(1) in two ways. First, under California law, both the Department and all child support agencies have the same right to access this type of information. By creating two separate subparts, the rule seems to suggest these two governmental entities may	

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			be.treated differently. This problem could be avoided by combining (b)(1)(B) an (b)(1)(J) into a single exception, . as follows: (b)(1)(B) California Department of Child Support Services *and local child support agencies:* family electronic records, child welfare electronic records, and parentage electronic records. Second, while it appears the JCC intends to ensure that the Department and LCSAs have electronic access to filings under Family Code Section 17404, and the Uniform Parentage Act (UPA), as provided by Family Code section 7643, the term "parentage" may be narrowly construed by some courts. As such, the Department respectfully requests that the term "parentage electronic records" be defined as follows:	

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			(b)(1)(B) California Department of Child Support Services *and local child support agencies:* family electronic records, child welfare electronic records, and parentage electronic records. *For purposes of this section, the term "parentage electronic records" includes, but is not limited to, any electronic record maintained by the court in any proceeding under: (1) the Uniform Parentage Act, to the extent permitted by Family Code Section 7643, (2) Family Code Sections 17400 and 17404, (3) the Uniform* *Interstate Family Support Act, or any of its predecessor laws, or (4) any other parentage proceeding, to the extent permitted by law.* The Department is also concerned that the rule, as drafted, might have other unintended	

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			consequences. In prior cycles, the JCC formally recognized through its adoption of the Notice of Change of Responsibility for Managing Child Support Case (Governmental) (FL-634) that LCSAs are able to enforce orders established in other counties now that there is a single statewide child support computer system and that such practice helps ensure there is no interruption in the flow of payments to families, particularly those that move from county to county on a regular basis. It is important that ***all*** local child support agencies have the ability to view California court records in different counties remotely. To avoid a misapplication of this rule, the proposed wording of Rule 2.540(b)(1)(J), referencing 'local child support agency' singular, may lead to confusion regarding whether an LCSA may seek remote access to court records for a court located in another county; thus, we recommend that the	

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			word "agency" be changed to "agencies" as stated above. The Department appreciates the addition of a good cause exception. It is noted that the LCSAs often have to file liens in civil and probate actions to secure payments for families. This good cause exception should make it clear to trial courts that they should not be restricting access to these case types in situations where it has already approved access to the Department and the LCSAs. It also encourages trial courts that are in the process of upgrading their current court case management system to develop it in a way that would permit the Department and the LCSAs to have increased access to these types of records. Finally, it is noted that the child support program has cooperative agreements with the JCC to provide funds to the trial courts to support their ability to provide	

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			remote access to the Department and the LCSAs. This cooperative agreement is supported by Title 45, Code of Regulations, section 302.34. In light of this relationship, the Department respectfully requests the JCC add a new subdivision to Rule 2.540, or alternatively add clarifying language to Rule 2.540(b)(1)(B), as follows: Nothing in this rule shall be construed to give courts the authority to impose remote access fees on any governmental entity receiving federal funds, either directly or indirectly, in accordance with Title 45, Code of Regulations, section 302.34.	
3	California Lawyers Association, by The Executive Committee of the Trust and Estates Section of CLA 180 Howard Street, Suite 410 San Francisco, CA 94105	AM	The Executive Committee of the Trusts and Estates Section of the California Lawyers Association (TEXCOM) supports the purpose and the general detail of the proposed changes to California Rules of Court,	The committee appreciates the comments. The suggested language provides clarity and will be added to the rule.

Positions: A = Agree; AM = Agree if modified; N = Do not agree; NI = Not indicated

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
	TEXCOM Ellen McKissock Hopkins & Carley Tel: 408-286-9800 E-mail: emckissock@hopkinscarley.com California Lawyers Association Saul Bercovitch Director of Governmental Affairs California Lawyers Association Tel: 415-795-7326 E-mail: saul.bercovitch@calawyers.org		rules 2.500-2.507 and the addition of rules 2.515 through 2.258. However, TEXCOM believes that the purpose of the new rules would be clearer if that purpose was actually stated in the Rules of Court, rather than in the Advisory Committee Comment. Practitioners will rely upon the actual rules set forth in the Rules of Court to understand the difference between the new "Article 2 Public Access" and the new "Article 3 Remote Access by a Party, Party Designee, Party's Attorney, Court Appointed Person." At present, we do not locate a statement in any of the rules that simply clarifies that Article 3 is intended to apply to the electronic records where remote access by the general public *is not* allowed (i.e. to the ten categories in Rule 2.507). To understand what Article 3 applies to, one must read the Advisory Committee Comment. Therefore, TEXCOM recommends that proposed rule 2.515 be revised as follows: **Rule 2.515 Application and scope**	

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			(a) No limitation on access to electronic records available through article 2 The rules in this article do not limit remote access to electronic records available under article 2. **These rules govern access to electronic records where remote access by the public is not allowed.** Without this clarification, members of TEXCOM initially read these new rules as creating additional hurdles and restrictions, and were opposed to the new rules. After reading the Advisory Committee Comments, TEXCOM understood the intent and supports the proposal if this clarification is made.	
4	Timothy Cassidy-Curtis 4467 Lakewood Blvd. Lakewood, CA 90712 Email: tcassidycurtis@roadrunner.com	AM	While all information, particularly personally identity information (PII) needs to be protected, it is also important to allow persons to electronically access all records that pertain to them. A particular example is the Application of petitioners for Change of Name. Our society is highly mobile,	The committee appreciates the comment. The proposed rules do not require the courts to certify electronic records to which they provide remote access though courts could do so, within their discretion, in light of statutory authority to certify electronic records under Government Code section 69150(f).

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			therefore electronic access of such records is essential, particularly when these records are to support further requests for personal documentation, such as birth certificates, etc. In my case, I am seeking my birth certificate from the State of New York. However, because I successfully petitioned to change my name (due to marriage; I am male, so that was the only option available) it becomes necessary to obtain original or certified court records regarding the petition to change my name. As you can imagine, travel to Santa Barbara would entail some difficulties, and an expenditure of energy that could be avoided with concurrent contribution to conservation along with avoidance of pollution and avoidance of Carbon Dioxide emissions. After several moves, the original issued by the court (it's been several decades!) becomes a problem. In the end, we need to be able to depend on the Court to provide certified records that pertain to us, in electronic format, or at least	

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			make an order (with, possibly, some payment to defray Court's costs), with a certified document mailed to us. All these reasons should support a very thorough conversion of records to electronic format, for production/publication as needed by persons to whom they pertain. Thank you for listening.	
5	Orange County Bar Association By Nikki P. Miliband, President P.O. Box 6130 Newport Beach, CA 92658 Tel: 949-440-6700 Fax: 949-440-6710	N	The OCBA is opposed to these Rule of Court amendments because they are unnecessary, possibly unconstitutional, contradictory, and well beyond the "limited" amendments referenced in the Executive Summary. The OCBA responds to the requests for specific comments as follows: (a) the proposal does not appropriately address the stated purpose because it merely creates unnecessary complexity to an area of law already governed by constitutional issues, freedom of the press, rights of privacy, access to justice and other	The committee appreciates the comments. It is unclear to the committee about what is unconstitutional or contradictory about the rules in the proposal. Not all records are remotely accessible by the general public by design to strike a balance between privacy and remote access. No members of the media submitted comments. A media entity's attorney would have the same level of access as any other attorney representing a party in a case under the new rules.

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			issues not susceptible to these specific proposals; (b) the remainder of the requests merely demonstrate the problems with this proposal – the general rules for open public access should not be so limited and restricted as set froth, it appears that the rules for a party's or attorneys access are more contrained than the general public and why should not other attorney's not involved in the case be allowed full access for purposes of investigation, research, background, due diligence, education, etc? The media will also have problems with these proposals because it is unclear whether their attorneys fall under the "general public" rules or the "party and party attorney" exceptions which appear to limit open access. Rule 2.501(b) appears to grant individed trial courts rights to further define and limit access which defeats the very purpose of these proposed "uniform" rules.	Regarding the amendment to rule 2.501(b), that rule only addresses providing plain language information to the public about access to electronic records. The new provisions governing remote access in article 3 and 4 provide for authority and responsibility of the courts. Those provisions broaden the opportunities to provide remote access. Regarding the amendments to rule 2.503(e), the comment is outside the scope of this proposal, as it is unrelated to the proposed amendments. The proposed amendments make only technical changes to the existing rule. The comments on articles 3 and 4 are broad and conclusory. The committee cannot formulate a response without more information on the conclusions in the comments.

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			Rule 2.503(e) outlines unnecessary and legally untenable restrictions and access to undefined "extraordinary criminal cases." The rule is confusing, unnecessary, and probably discriminatory and unconstitutional. The entirety of Article 3 regarding access by a party, party designee, party attorney, court-appointed person, or "authorized person working in a legal organization" appears to be unnecessary, too redundant, too restrictive, and probably discriminatory. The entirety of Article 4 has the same problems as Article 3 and suffers again from being unnecessary for these purposes.	
6	Superior Court of California, County of Orange By Cynthia Beltrán, Administrative Analyst Family Law and Juvenile Court	NI	**What would the implementation requirements be for courts?** *This is dependent upon whether or not courts have existing applications that allow remote access.*	The committee appreciates the responses to the request for specific comments and they are helpful, providing needed information to the committee.

Positions: A = Agree; AM = Agree if modified; N = Do not agree; NI = Not indicated

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
	Tel: 657-622-6128 E-mail: cbeltran@occourts.org		**What implementation guidance, if any, would courts find helpful?** *A quick reference* **Should proposed rule 2.518 be limited to certain case types?** *Yes, the rule should be clear that it does not apply to juvenile justice and dependency case types.* **Would an alternative term like "preliminary legal services" be more clear?** *Yes. Is the intention to allow attorneys on a case to have permanent access or is there an expectation the court must manage limited-time access to those that are given consent? Similar to restricted access for designees. Additionally, once consent is given by a party for others to have access do you intend to create a process for them to retract consent?* **Is the term "legal organization" and its definition clear or necessary?** *Yes, it is clear and necessary.*	Regarding rule 2.518, if the concern is that a designee may obtain confidential information, the designee level of remote access is only to the same information the public could get at the courthouse. Information that is not available to the general public at the courthouse will not be remotely accessible by the designee. Regarding brief legal services and time limited consent, there is not an expectation that courts must manage limited-time access except for the party designees under rule 2.518 where a party may limit a designees access to a specific period of time, limit access to specific cases, or revoke access at any time. The process would be expected to be built into the system. Otherwise, the scope of consent in the context of a qualified legal services project providing brief services would be dictated by agreement between the party and the organization.

Positions: A = Agree; AM = Agree if modified; N = Do not agree; NI = Not indicated

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			Would referring to persons "working at the direction of an attorney" be sufficient? *No, that is too broad of a definition.* **Is "concurrent jurisdiction" the best way to describe such cases or would different phrasing be more accurate?** *Concurrent jurisdiction should be defined within the rule itself.* **Is the standard for "good cause" in proposed rule 2.540(b)(1)(O) clear?** *Yes* **Would the proposal provide cost savings?** *No, the administration of managing remote access and unique credentials under these rules will result in ongoing-additional costs. Maintenance of restricted and/or limited term access to remote information will be necessary and require someone to control.*	Need committee responses here and immediately below. Make sure the responses align with the comments throughout this chart. The comments on costs will be included with the Judicial Council report.

Positions: A = Agree; AM = Agree if modified; N = Do not agree; NI = Not indicated

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			Managing user ID's and password control should also be considered. guide for courts to reference when developing remote access applications would be helpful.	
			Would providing limited audit trails to users under rule 2.256 present a significant operational challenge to the court? *This is more of a technical challenge more than an operational challenge. Clarification would be needed on what a limited audit trail is or what the purpose is in providing it to authorized users. While it says the limited audit trail must show the user who remotely accessed electronic records, it is uncertain what the reason a remote access user needs to see who else accessed the record. It is recommended additional information be included in this rule to clarify the intent of providing a limited audit trail.*	The committee will add an advisory committee comment explaining the purpose of the audit trail.

ITC SPR18-37
Technology: Remote Access to Electronic Records

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
7	Superior Court of California, County of Orange, West Justice Center By Albert De La Isla, Principal Analyst IMPACT Team – Criminal Operations Tel: 657-622-5919 Email: adelaisla@occourts.org	NI	For courts that already provide electronic remote access to defense and prosecutors / law enforcement, would we have to go back and re-certify each access as well as have them sign user forms?	To the extent remote access is already being provided consistent with the rules, there is no need to re-do any certifications or user agreements. If remote access is provided that is not compliant with the rules then the courts should take necessary steps to become compliant. Note that the rules do not prescribe any particular method for identity verification or capturing consent. This could be done through agreements between the government entities and the court (e.g., the government entities will have almost certainly verified the identities of their own employees and can confirm that is authorized users are who they say they are).
8	Superior Court of Placer County By Jake Chatters Court Executive Officer 10820 Justice Center Drive, Roseville, CA 95678 P. O. Box 619072, Roseville, CA 95661 Tel: 916-408-6186	AM	The Placer Superior court appreciates the opportunity to comment on the proposed California Rules of Court 2.515-2.528 and 2.540-2545 and amended rules 2.500-2.503 for the remote access to court records.	The committee appreciates the feedback. Please see the committee response to the TCPJAC/CEAC comments.

Positions: A = Agree; AM = Agree if modified; N = Do not agree; NI = Not indicated

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
	Fax: 916-408-6188		The Trial Court Presiding Judges' Advisory Committee (TCPJAC) and the Court Executive Advisory Committee (CEAC) have submitted comments that support this proposal but request clarifying amendments. Our court joins TCPJAC/CEAC in their comments. We are pleased to offer our agreement with the rule changes, while encouraging the Committee to consider the amendments proposed by TCPJAC/CEAC. Thank you again for the opportunity to comment.	
9	Superior Court of San Bernardino County By Executive Office ExecutiveOffice@sb-court.org	NI	The proposal makes limited amendments to rules governing public access to electronic trial court records and creates a new set of rules governing remote access to such records by parties, parties' attorneys, court-appointed persons, authorized persons working in a legal organization or qualified legal services project, and government entities. The purpose of the proposal is to facilitate existing relationships	Regarding the comment about CASAs, the remote access rules do not alter confidentiality requirements to juvenile court records. That would require legislative and rule-making action that is beyond the scope of this proposal.

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			and provide clear authority to the courts. The project to develop the new rules originated with the California Judicial Branch Tactical Plan for Technology, 2017–2018. Under the tactical plan, a major task under the "Technology Initiatives to Promote Rule and Legislative Changes" is to develop rules "for online access to court records for parties and justice partners." (Judicial Council of Cal., California Judicial Branch Tactical Plan for Technology, 2017–2018 (2017), p. 47.) In the term "Brief Legal Services", the juvenile courts provide access to "CASA Volunteers" who are appointed to the minor and are an integral part of the juvenile court. The issue is when the minors become "Non-Minor" dependents and CASA is not allowed to view their delinquency file either electronically or in paper, without the minors approval (1/1/2019).	

Positions: A = Agree; AM = Agree if modified; N = Do not agree; NI = Not indicated

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			Comments: Level of Remote Access: Appointed Counsel other than the public defender is not listed, i.e. counsel for minors or parents in Dependency Court. i.e. the "conflict panel" for delinquency and dependency attorneys should be included, along with Guardian Ad Litems that are appointed in juvenile court matters.	Tthe committee assumes the comment is in reference to rule 2.540(b), which is the only rule that mentions public defenders in particular. That rules is part of article 4, which governs remote access by government entities to specified records. Entities that do not meet the definition of "government entity" will not fall within the scope of that rule. Court-appointed persons and attorneys for parties would gain access under the rules of article 3.
10	Superior Court of California, County of San Diego By Mike Roddy, Executive Officer 1100 Union Street San Diego, CA 92101	AM	Q: Does the proposal appropriately address the stated purpose? Yes. Q Proposed rule 2.518 would allow a person who is a party and at least 18 years of age to designate other persons to have remote access to the party's electronic records. What exceptions, if any, should apply where a person under 18 years of age could designate another? An emancipated or married minor should be exceptions for a person	The committee appreciates the responses to the request for specific comments. They are helpful and insightful information for committee to consider.

Positions: A = Agree; AM = Agree if modified; N = Do not agree; NI = Not indicated

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			under 18 years of age. Additionally, should an exception be made for someone who is over 18 years of age but under a Conservatorship? Q Should proposed rule 2.518 be limited to certain case types? No. Q The term "brief legal services" is used in the proposed rules in the context of staff and volunteers of "qualified legal services organizations" providing legal assistance to a client without becoming the client's attorney. The rule was developed to facilitate legal aid organizations providing short-term services without becoming the client's representative in a court matter. Is the term "brief legal services" and its definition clear? Would an alternative term like "preliminary legal services" be more clear? The proposed "brief legal services" is clear and preferred over "preliminary legal services." Preliminary makes it sound like it	The committee appreciates the point concerning the age cut off in rule 2.518 as it appears it is a standard that is both under and overinclusive.

Positions: A = Agree; AM = Agree if modified; N = Do not agree; NI = Not indicated

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			would only be during the case initiation phase, when in reality they could obtain assistance throughout the life of a case. Q Is the term "legal organization" and its definition clear or necessary? The proposed "legal organization" is clear. Q Rather than using the term "legal organization" in rule 2.520, which covers remote access by persons working in the same legal organization as a person's attorney, would referring to persons "working at the direction of an attorney" be sufficient? The definition is clear and it is helpful to include the list of examples, such as partners, associates, employees, volunteers and contractors. The alternative suggested is too broad with room for interpretation. Q The reference to "concurrent jurisdiction" in proposed rule 2.540(b)(1)(N) is intended to	

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			capture cases in which a tribal entity would have a right to access the court records at the court depending on the nature of the case and type of tribal involvement. Is "concurrent jurisdiction" the best way to describe such cases or would different phrasing be more accurate? The phrase "concurrent jurisdiction" is sufficient to describe these scenarios. Q Is the standard for "good cause" in proposed rule 2.540(b)(1)(O) clear? Yes. Q The proposed rules have some internal redundancies, which was intentional, with the goal of reducing the number of places someone reading the rules would need to look to understand how they apply. For example, "terms of remote access" in article 3 appears across different types of users to limit how many rules a user would need to review to understand certain requirements. As another example,	

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			rules on identity verification requirements appear in articles 3 and 4. Does the organization of the rules, including the redundant language, provide clear guidance? Would another organizational scheme be clearer? The included language is clear and reduces the need for the user to refer to additional rules. Q: Would the proposal provide cost savings? No. Q: What would the implementation requirements be for courts—for example, training staff (please identify position and expected hours of training), revising processes and procedures (please describe), changing docket codes in case management systems, or modifying case management systems? In order to be able to answer this question, our court has identified the following issues:	The comments on costs and implementation will be included with the Judicial Council report.

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			1. Our court needs to understand the business and technical requirements of the implementation. For example, we need to understand the audience that will need access. Will each group of the audience have the same or unique access requirements. For example, do we need to restrict access from specific networks. 2. Audit and security requirements. Our court needs to be able to generate reports on who, where, when and how long the application was used by remote users. 3. Testing. Our court needs to be able to identify the testing requirements, especially if the level of access for each audience is different. There needs to be participation from the justice partners (i.e. government agencies). 4. Training. Tip sheets will need to be prepared for the users. 5. Legal. There needs to be some kind of MOU with the remote user\justice partner. Q: What implementation guidance, if any, would courts find helpful?	

Positions: A = Agree; AM = Agree if modified; N = Do not agree; NI = Not indicated

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			A governance and best practice checklist for implementing remote access. Q: The audit trail requirements are intended to provide both the courts and users with a mechanism to identify potential misuse of access. Would providing limited audit trails to users under rule 2.256 present a significant operational challenge to the court? If so, is there a more feasible alternative? No. The conditions stated in rule 2.256 are sufficient. <u>General Comments:</u> **2.521(a)(2):** Suggests that the following citations be added for appointment of an attorney in Probate: Probate Code §§ 1894, 2253, and 2356.5 **2.540(b):** Proposes that Public Administrator and Public Conservator be added to the list of authorized persons from government entities that may be	The committee declines to add the additional citations they do not confer separate, independent authority or duty on the court to appoint. The committee will recommend a proposal be developed for future rules cycle to add the public administrator and public conservator. In the interim, courts can use the "good cause" provision to provide access.

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			provided remote access to electronic records.	
11	Superior Court of California, County of San Joaquin Erica A Ochoa Records Manager 540 E Main Street Stockton CA 95202 Tel: 209-992-5221 eochoa@sjcourts.org	NI	Does the proposal appropriately address the stated purpose? • Proposed rule 2.518 would allow a person who is a party and at least 18 years of age to designate other persons to have remote access to the party's electronic records. What exceptions, if any, should apply where a person under 18 years of age could designate another? I think you should match the age guidelines applied to filings such as DV/CH orders. If a person, legislatively can file then they should have the right of assigning a designee of their choice to access their records. I believe the age is 12. • Should proposed rule 2.518 be limited to certain case types? If you do not limit now, you will have a much more difficult time limiting later. It is safer to begin limited and slowly release additional information. Once you have given	The committee appreciates the responses to the specific comments as they are helpful in determining the committee's recommendation to the council. The committee declines to reduce the age to 12. Ultimately, the user must have the legal capacity to agree to be bound by the terms and conditions of user access.

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			unlimited access it is very difficult to convince the public you are not hiding something by taking choices away. The question of transparency will be front and center rather than the right to protect information. • The term "brief legal services" is used in the proposed rules in the context of staff and volunteers of "qualified legal services organizations" providing legal assistance to a client without becoming the client's attorney. The rule was developed to facilitate legal aid organizations providing short-term services without becoming the client's representative in a court matter. Is the term "brief legal services" and its definition clear? Yes it is. Would an alternative term like "preliminary legal services" be more clear? No, I think it would be more confusing.	

Positions: A = Agree; AM = Agree if modified; N = Do not agree; NI = Not indicated

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			We often try to read between the lines to properly interpret and understand the intent behind a lot of legislation and/or rules. Describing these temporary services as "brief" rather than "preliminary" makes it clearer as to their involvement in the case. • Is the term "legal organization" and its definition clear or necessary? Yes it is and yes it must, without it any organization can make the plea for access whether or not they are party to the case. • Rather than using the term "legal organization" in rule 2.520, which covers remote access by persons working in the same legal organization as a person's attorney, would referring to persons "working at the direction of an attorney" be sufficient? Yes it would and would add clarity to the rule.	

Positions: A = Agree; AM = Agree if modified; N = Do not agree; NI = Not indicated

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			• The reference to "concurrent jurisdiction" in proposed rule 2.540(b)(1)(N) is intended to capture cases in which a tribal entity would have a right to access the court records at the court depending on the nature of the case and type of tribal involvement. Is "concurrent jurisdiction" the best way to describe such cases or would different phrasing be more accurate? No, I think it is confusing because it gives the impression both courts have agreed jurisdiction is shared when it may not necessarily be. We can apply the rule if the description remained the same as other government agencies and remove the word "concurrent". • Is the standard for "good cause" in proposed rule 2.540(b)(1)(O) clear? Yes, it is. • The proposed rules have some internal redundancies, which was intentional, with the goal of reducing the number of places	

Positions: A = Agree; AM = Agree if modified; N = Do not agree; NI = Not indicated

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			someone reading the rules would need to look to understand how they apply. For example, "terms of remote access" in article 3 appears across different types of users to limit how many rules a user would need to review to understand certain requirements. As another example, rules on identity verification requirements appear in articles 3 and 4. Does the organization of the rules, including the redundant language, provide clear guidance? Yes, it does. Would another organizational scheme be clearer? No additional comment. • Would the proposal provide cost savings? If so, please quantify. In the long run there may be some savings due to less walk-in customers at local courthouses however the costs associated to comply with all levels of identity verification and access will create additional ongoing costs for the	Comments on the costs and implementation will be included with the Judicial Council report.

Positions: A = Agree; AM = Agree if modified; N = Do not agree; NI = Not indicated

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			court. There will also be additional ongoing costs for the addition of staff to monitor, manage, and update all changes required to comply with the identity verification and audit trail requirements. We cannot quantify the savings as we cannot predict the amount of public who will have the means to access court records remotely nor do we know the exact amount of employees needed to maintain these requirements. • What would the implementation requirements be for courts—for example, training staff (please identify position and expected hours of training), revising 12 processes and procedures (please describe), changing docket codes in case management systems, or modifying case management systems? There will be a level of training necessary to implement a process such as this but it is not possible to specify the exact amount of time necessary to execute all processes.	

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			For example, in our court, time and cost must be invested to: • Set up, testing, training, and implementation of an additional program because our current case management system is not set up to handle the identity and audit trails required in the amendment. • Create and train staff assigned to monitor and manage the additional program for questions from the public, account set-up, password management, and any other situation arising from user end regarding remote records access. • What implementation guidance, if any, would courts find helpful? Provide all the information for the Service Master agreement as soon as possible to allow courts to reach out to vendors and explore the on-going cost, time investment, maintenance, in order to determine	

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			if it is feasible for the court to follow through with implementation of remote records access. • The audit trail requirements are intended to provide both the courts and users with a mechanism to identify potential misuse of access. Would providing limited audit trails to users under rule 2.256 present a significant operational challenge to the court? Yes it would. Allowing ad-hoc report requests is new to our organization and would require staff, time, and on-going costs in order to maintain the ability to create these reports. If so, is there a more feasible alternative? Require the customer to provide good cause for a report to be created and allow us to determine how and when to create these reports for the purpose of auditing the system to ensure proper usage.	The committee declines to add "good cause" language. The committee has instead made the audit trail permissive rather than mandatory.

ITC SPR18-37
Technology: Remote Access to Electronic Records

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
12	TCPJAC/CEAC Joint Rules Subcommittee (JRS) By Corey Rada, Senior Analyst Judicial Council and Trial Court Leadership | Leadership Services Division Judicial Council of California 2860 Gateway Oaks Drive, Suite 400 Sacramento, CA 95833-3509 Tel. 916-643-7044 E-mail: Corey.Rada@jud.ca.gov www.courts.ca.gov	AM	The following comments are submitted by the TCPJAC/CEAC Joint Technology Subcommittee (JTS) on behalf of the Trial Court Presiding Judges Advisory Committee (TCPJAC) and the Court Executives Advisory Committee (CEAC). **SPR18-37:** Recommended JTS Position: Agree with proposed changes if modified. JTC recognizes the need for changes to the existing remote access to electronic records rules. On balance, the changes recommended by ITAC present necessary clarifications to the rules and establish reasonable requirements for accessing court records. However, JTS notes the following impact to court operations: • The proposal will create the need for new and/or revised procedures and alterations to case	The committee appreciates the comments. The comments on impacts on case management systems, workload, and security will be included with the Judicial Council report. Regarding rule 2.502(4), the suggested modification is clearer and the committee has made this change. Regarding rule 2.503(b)(2), the suggested modification will be made as a technical correction. Regarding rule 2.516, the committee agrees to add an advisory committee comment clarifying that different user types can be added as it becomes feasible to do so. The committee did not intend for the rules to require the courts to proceed in an "all or none" fashion with respect to the users identified in rule 2.515. Regarding rule 2.518, the committee declines to add a statement that

Positions: A = Agree; AM = Agree if modified; N = Do not agree; NI = Not indicated

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			management systems. A number of proposed revisions in the proposal would present a workload burden on the trial courts, create new access categories that will result in significant one-time or ongoing costs, and complicate the access rules in a way that may result in confusion for the public. • Increases court staff workload – Court staff would be required to verify the identity of individual(s) designated by the party to access their case. • Security – The proposed changes could result in security complications and allow for data intrusion. *Suggested Modifications:* • **Rule 2.502 Definitions** o Modify the definition of "court case information" to use more natural language to reduce confusion. A possible definition might be:	providing remote access under rule 2.518 is optional because it is contrary to the intended scope of article 3. This type of remote access is not optional if it is feasible to provide it. If it is not feasible for a court to provide remote access to party designees (e.g., court does not have the financial resources, security resources, technical capability, etc.), courts do not have to provide it. The committee declines to add a rule that a party must make an affirmative declaration absolving the Judicial Branch of liability, such a rule is unnecessary. Courts can include terms regarding liability in user agreements. Regarding rule 2.519(c), the rule was developed under the assumption that the rules of professional conduct would constrain attorneys from making misrepresentations to the court and that the court could rely on an attorney's representation of a party's consent. The challenge with limited scope representation in particular is that the attorney may be

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			"Court case information" refers to data that is stored in a court's case management system or case histories. This data supports the court's management or tracking of the action and is not part of the official court record for the case or cases. • **Rule 2.503(b)(2)** o "All records" should be "All court records." By excluding the term "court" in this section, it seems that the public access may be expanded beyond "court records." • **Rule 2.516 Remote access to the extent feasible** o The language makes clear that courts may provide varied remote access depending on their capabilities. However, as written it is unclear whether it is ITAC's intent that courts refrain from moving forward with any part of the remote access options until they can move forward with all of the	unknown to the court. Attorneys providing limited scope representation under chapter 3, of title 3 (the civil rules), are permitted to provide noticed representation or undisclosed representation. Requiring an attorney to file a notice of limited scope representation requires notice and service on all parties. (Rule 3.36(h).) Being required to provide noticed representation could add costs to the party who only require assistance in the drafting of legal documents in their matters, or require assistance with collateral matters. It is not clear what the benefit would be of requiring attorneys to file a notice of limited scope representation or declaration of representation on appeal over requiring an attorney to "represent [] to the court in the remote access system that the attorney has obtained the party's consent to remotely access the party's electronic records." That representation is how

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			options. To avoid confusion and/or unnecessary delays in implementation of some portions of remote access, the rule could be modified to add: *Courts should provide remote access to the greatest extent feasible, even in situations where all access outlined in these rules is not feasible.* Alternatively, or in addition, we ask that ITAC consider adding a statement to the Advisory Committee Comment to indicate: "This rule is not intended to prevent a court from moving forward with limited remote access options outlined in this rule as such access becomes feasible." • **Rule 2.518 Remote access by a party's designee** TCPJAC and CEAC strongly encourages ITAC to amend this provision. TCPJAC/CEAC offers the following additional comments: ▪ Add a statement making clear that the provision of this type	the court would know that consent had been given. TCPJAC/CEAC raise a concern that remote access under (c) "might include documents that are not publicly viewable." This should not be the case. An attorney providing undisclosed representation is still limited by the information that the attorney could get at the courthouse. If an attorney providing undisclosed representation showed up at the courthouse, he or she could access any public court records. The remote access rules are replicating that. What rule 2.519(c) does is allow remote access to materials that is only available to the public at the courthouse under rule 2.503(c). In short, with respect to attorneys who are unknown in the case because their representation is undisclosed, the remote access is to public court records. An attorney providing undisclosed representation should not be able to view documents that are not publicly viewable. The committee added additional

Positions: A = Agree; AM = Agree if modified; N = Do not agree; NI = Not indicated

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			of access is optional and not a mandate on the trial courts. ▪ Add a rule that the party must make an affirmative declaration that by granting their designee access to their case file, the trial court and the Judicial Branch are absolved of any responsibility or liability for the release of information on their case that is inconsistent with this or other rules or laws. • **Rule 2.519(c) Terms of remote access for attorneys who are not the attorney of record in the party's actions or proceedings in the trial court** o This rule presents a significant security risk to court data and could add an additional burden on the court. This section appears to contemplate giving access to case information that is otherwise not publicly available, to attorneys who have not formally appeared or associated in as counsel in the case. It is	information to the advisory committee comment to clarify this point. TCPJAC/CEAC raises concerns that (c) also increases the risk of a data breach and wrongful access and has requested that (c) be optional on the part of the court. The remote access to users in article 3 is not meant to be optional, but rather required if feasible. It is not clear why the feasibility qualification would not be sufficient to address this, e.g., if it is not feasible for the court to provide adequate protections against data breaches then it would not be required, or if it is not feasible for the court to provide differential access to attorneys of record vs. other attorneys who have party consent then it would not be required. The revision to the advisory committee comment on rule 2.516 concerning feasibility makes clear that having adequate security resources can be part of whether providing users access is feasible.

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			unclear how the party would inform the court of their consent to have the attorney access the case information, which might include documents that are not publicly viewable. It is also unclear how the court would verify the identity of the attorney who is not of record in this process. If this provision remains, the attorney access should be significantly limited. For example, fair and reasonable access can be accomplished by requiring an attorney to file notice of limited scope representation. Similarly, an appellate attorney representing the party on an appeal relating to the action may be provided access upon declaration that the attorney is attorney of record in appellate proceedings. Additionally, attorneys providing brief legal services are provided access otherwise in these rules. To expand the attorney access to any attorney granted permission by the party would overly burden the court and	The commenters also state that "It is also unclear how the court would verify the identity of the attorney who is not of record in this process." By design, the rules do not prescribe any specific method for a court to use for identity verification. It is something the court could do (e.g., require an attorney to appear at the court and show their identification and bar card to get user credentials), require a legal organization or qualified legal services project to do (e.g., require in an agreement that the organization to do identity verification of its attorneys and staff and provide that information to the court), or contract with an identity verification service to do (e.g., a private company that is in the business of identity verification). A court must verify identities to provide remote user access under article 3, but if not feasible to do so, then the court does not need to provide the remote access.

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			appears unnecessary. Further, each additional tier of data access presents additional risk of data breach or the potential for bad actors to exploit access. TCPJAC and CEAC strongly encourage ITAC to amend this provision and offer the following additional comments: ▪ Add that the attorney file appropriate documentation of limited scope representation. ▪ Add a statement making clear that the provision of this type of access is optional and not a mandate on the trial courts. ▪ Add a rule that the party must make an affirmative declaration that by granting their designee access to their case file, the trial court and the Judicial Branch are absolved of any responsibility or liability for the release of information on their case that is inconsistent with this or other rules or laws. • **Rule 2.520 Remote access by persons working in the same**	The comment about the release of liability relates to the party designee rule (rule 2.518) and is addressed in the analysis with that comment. Regarding 2.520, the committee agrees to add the advisory committee comment. The rules do not require any specific process. Certifying at one time and having that time be when an attorney establishes a remote access account is a logical and practical option. Regarding rule 2.522, the comment notes, that "this section appears to exempt these agencies from the limitations of remote access to cases defined in rule 2.503(c). The purpose of granting this exemption is unclear…" This section does exempt qualified legal services projects from the limitations of rule 2.503 in that qualified persons from a qualified legal services project may remotely access the court records accessible by the public only at the courthouse, specifically, those records outlined in rule 2.503(c).

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			legal organization as a party's attorney. o We suggest adding an Advisory Committee Comment that the designation and certification outlined in (b) need only be done once and can be done at the time the attorney establishes their remote account with the court. • **2.522 Remote access by persons working in a qualified legal services project providing brief legal services.** o As written, this section appears to exempt these agencies from the limitations of remote access to cases defined in rule 2.503(c). The purpose of granting this exemption is unclear, particularly in light of the other additions to the rule. For example, if rule 2.518 is adopted, this section may be unnecessary. Similarly, if rule, 2.519 is adopted, this section again may be unnecessary. Further, if rules 2.518 and 2.519 are not adopted, this rule presents additional concerns:	The purpose of the exemption is to provide remote access where remote access is otherwise precluded under the public access rules. The rule does not alter the content of the court records that can be accessed, only the method. The comments state, "For example, if rule 2.518 is adopted, [rule 2.522] may be unnecessary." The committee disagrees. Rule 2.518 provides an alternative, but parties who do not have the ability to do access the system to provide designees, e.g., lack computer or internet access or lack the skills to access, would not be able to designate persons working at a qualified legal services project. Qualified legal services projects, like legal aid, serve populations with limited access to resources that may not be able to designate another under rule 2.518. The comments also state, "Similarly, if rule, 2.519 is adopted, [rule 2.522] again may be unnecessary." The

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			▪ 2.522(b) requires the legal services project to designate individuals in their organization who have access, and certify that these individuals work in their organization. It is unclear whether this designation and certification is provided to the court or retained by the organization. It is also unclear whether this designation or certification is one-time, repeated, or must occur upon each access to a case. ▪ 2.522(d)(1) states that the organization must have the party's consent to remotely access the party's record. It is unclear how such consent would be documented. ▪ 2.522(d)(2) creates a specific technical requirement that courts would have to program into their remote access systems that requires a self-representation of consent each time the authorized person accesses a case. Unlike the other provisions of these rules, that appear to contemplate a one-time designation, this section would	committee disagrees. Rule 2.519 is attorney access. A person working in a qualified legal organization may not be an attorney, e.g. paralegal or intern. An attorney at a qualified legal services project may never end up providing representation. Regarding the comments on rule 2.522(b) and 2.522(d)(1), the committee will add an advisory committee comment to clarify. Courts and qualified legal services projects have flexibility to determine methods that work best for them. Regarding the comments on rule 2.522(d)(2), the committee agrees that remote access could present a greater technical challenge. A court does not have to provide remote access to users under rule 2.522 if it is not feasible to do so, e.g., because the court's technical capacity makes it not feasible at present. Regarding rule 2.523, the committee agrees with exempting courts from verifying the identities of users

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			require an entirely new security layer at a "session" level to ensure the authorized individual continues to certify their authorization to access the case. • **Rule 2.523 – Identity verification, identity management, and user access** o This section requires the court to verify the identity of all users accessing court data. This requirement is understandable when it relates to individuals who are known to the court to be a part of the case being accessed. However, placing a requirement on the court to verify the identity of individuals designated by the party to access their case is overly burdensome and places the court in the position to verify the identity of individuals unknown to the court. We suggest adding language to clarify that the court is not required to verify the identity of individuals granted access under rule 2.518, 2.519, and 2.522 (if those sections remain). These rules grant access to	gaining remote access as party designees under rule 2.518. The committee disagrees with exempting courts from verifying the identities of users under rule 2.519 and rule 2.522. Rule 2.519 has a mix of known and unknown persons (attorneys who have made an appearance, and attorneys who are undisclosed). Rule 2.522 will have persons unknown to the court. The identity verification process is meant to provide a way for unknown persons to be known and to verify that known persons are who they say they are. The rule is meant to be flexible in how a court verifies identities and it could be done by the court or through agreements with third parties, e.g., an agreement with a company that provides identity verification services, or an agreement with a qualified legal services project that the project is required to verify the identities and provide that verification to the court (it is likely that with respect to its own employees, a qualified legal services project would have already

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			cases by individuals unknown to the court based solely upon the consent of the party or by designation of third-parties. Under these conditions, the party is consenting to access and the court should have no responsibility to perform identify verification. Further, as previously stated, in all such instances, the rules should clearly state that the party is removing the court's responsibility for data security and confidentiality. o Subsections (a) and (d) appear to be in minor conflict. Suggest adding an indication that (d) applies notwithstanding (a). • **Rule 2.524 Security of confidential information.** o We suggest adding an Advisory Committee Comment that specifies that data transmitted via HTTPS complies with the encryption requirement. • **Rule 2.526 Audit trails**	done its due diligent to verify that a person is who they say they are). In addition, rule 2.523(c) puts the onus on the person seeking remote access to provide the court with all information it directs in order to identify the person. The court is not obligated to seek out information about the person. If the information a person provides is insufficient to verify their identity, the court is not obligated to provide remote access. The committee does not believe subdivisions (a) and (d) are in conflict, but the commenter may interpret them as imposing on the court an obligation to take additional steps to verify identities beyond what a legal organization or qualified legal services project has done. However, (a) is not requiring duplication of effort and (d) could satisfy (a). In other words, if a legal organization has verified the identity of potential remote user, a paralegal working at the legal organization named Jane Smith, and the legal

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			o Since these records would also be available at the courthouse, where no record of access is kept, the record keeping here seems to be unnecessary and burdensome. However, should ITAC choose to retain this section, we recommend it be modified as follows: *The court should have the ability to generate an audit trail that identifies each remotely accessed record, when an electronic record was remotely accessed, who remotely accessed the electronic record, and under whose authority the user gained access to the electronic record.* The current mandatory language may result in a court being prohibited from providing any electronic access even with the ability to do so, if the court does not have the ability to provide the required audit trail. We suggest changing "must" to "should" and adding an Advisory Committee Comment making clear this rule is not intended to eliminate existing	organization communicates that it has done so with the court, the court does not need to take further steps to verify Jane Smith's identity. The court would have verified Jane Smith's identity through the legal organization. The committee will add an advisory committee comment to clarify that (d) can satisfy (a). Regarding rule 2.524, the committee declines to add an advisory committee comment. The rules are intended to be technologically neutral and not tied to any particular technology. Rather than adding an advisory committee comment about specific technologies that will change over time, this may be better addressed through informational materials such as guidance documents or examples from courts. Regarding rule 2.526, the committee agrees to change the rule from mandatory to permissive in order to not stifle the use of existing systems. The committee will add an advisory committee comment that it expects

All comments are verbatim unless indicated by an asterisk (*)

#	Commentator	Position	Comment	Committee Response
			online services, but instead is intended to guide future implementations and upgrades to court remote services. This section would also benefit from a defined retention period for the audit records. ITAC may wish to establish a timeframe, e.g. one year, from the date of access or the disposition of the case as determined by the respective courts.	the rule will become mandatory in the future. This should accommodate existing systems while also encouraging the inclusion of audit trails as remote access systems are developed and improved. The committee agrees that a rule governing a retention period for audit trails may be helpful and that may be addressed in a future rule cycle so it may circulate for comment.
13	Tulare County Public Guardian's Office By Francesca Barela, Deputy Public Guardian, 3500 W. Mineral King Ave., Suite C, Visalia CA, 93291 Tel: 559-623-0650 Email: FBarela@tularecounty.ca.gov	A	The proposed changes clarify and expand on the existing rules. I personal approve of these changes.	The committee appreciates the support.