JUDICIAL COUNCIL OF CALIFORNIA

455 Golden Gate Avenue • San Francisco, California 94102-3688
Telephone 415-865-4200 • Fax 415-865-4205 • TDD 415-865-4272

MEMORANDUM

Date
June 25, 2018

To
Information Technology Advisory Committee
Hon. Sheila F. Hanson, Chair

From
Andrea L. Jaramillo
Attorney, Legal Services

Subject
Rules Proposal: Review public comments and make recommendation on amending Cal. Rules of Court, rules 2.250, 2.251, 2.252, 2.253, 2.254, 2.255, 2.256, 2.257, and 2.259

Action Requested
Please review

Deadline
July 2, 2018

Contact
Andrea L. Jaramillo
Legal Services
916-263-0991 phone
andrea.jaramillo@jud.ca.gov

Background

This spring, the Information Technology Advisory Committee (ITAC) circulated a rules proposal for public comment that would amend several rules related to electronic service and electronic filing found in title 2, division 3, chapter 2 of the California Rules of Court. New provisions of Code of Civil Procedure section 1010.6 (section 1010.6) require express consent for electronic service necessitate conforming changes to the rules of court. In addition, the new provisions of section 1010.6 require the Judicial Council to adopt rules of court related to disability access and electronic signatures for documents signed under penalty of perjury. Finally, the proposal includes amendments based on comments received from the public. These include amendments to the definitions and contract requirements between EFSPs and courts. The public comment period ended on June 8, 2018.

On June 21, 2018, the ITAC Rules and Policy Subcommittee also recommended the proposal for adoption by the Judicial Council.

Discussion

Four commenters responded to the invitation to comment either agreeing with the proposal or agreeing as modified. Three of the commenters responded with substantive comments focused on amendments to the definitions and requirements for express consent to electronic service.

A. Rule 2.250(b)(1) definition of "document"

Rule 2.250(b)(1) defines "document" as:

> a pleading, a paper, a declaration, an exhibit, or another filing submitted by a party or other person, or by an agent of a party or other person on the party's or other person's behalf. A document is also a notice, order, judgment, or other issuance by the court. A document may be in paper or electronic form.

The current wording of the definition of "document" can be read to mean that a document must be a filing. The proposed amendment removes this ambiguity by striking "filing" and replacing it with "writing" to clarify that a "document" is not necessarily a filing. When the Rules and Policy Subcommittee discussed circulating the proposal, it also struck the first use of the term "paper" in the definition as unnecessary.

The Superior Court of California, County of Los Angeles and the Trial Court Presiding Judges Advisory Committee/Court Executive Advisory Committee (TCPJC/CEAC) Joint Rules Subcommittee both submitted the same comment:

> The proposed definition allows confusion, inasmuch as it leaves open the possibility of a person e-filing a hearing exhibit, or trial exhibit. The language should explicitly exclude such exhibits from the definition in 2.250(b)(1), or allow courts to exclude them through local rules.

1. Subcommittee and staff review

The existing rule contains "an exhibit" within the scope of what can constitute a "document" and this is unaffected by the proposed amendments. The subcommittee considered that the concern may be because "writing" was added in the amended version and "writing" is an expansive term. The subcommittee required more information. Following the subcommittee meeting, staff contacted the commenter for additional information on which term was problematic. The

commenter verified that it was the use of "an exhibit" in the existing definition. The current rules do provide authority for courts to make local rules on electronic filing and the commenter noted that that would be sufficient to address the concern.

B. Rule 2.251 provisions for consent to permissive electronic service

Effective January 1, 2019, section 1010.6 will no longer allow the act of electronic filing alone to serve as consent to permissive electronic service. (§ 1010.6(a)(2)(A)(ii).) Under section 1010.6, parties may still consent through electronic means by "manifesting affirmative consent through electronic means with the court or the court's electronic filing service provider, and concurrently providing the party's electronic service address with that consent for the purpose of receiving electronic service." The proposal amends rule 2.251(b)(1)(B) to remove the provision allowing the act of filing to serve as consent to electronic service and replaces it with the language for manifesting affirmative consent by electronic means from section 1010.6.

1. Manifestation of affirmative consent

The proposal adds rule 2.251(b)(1)(C) to provide for how a party or other person may "manifest affirmative consent." To do so, a party other person would either (a) agree to the terms of service agreement with an electronic filing service provider, which clearly states that agreement constitutes consent to receive electronic service electronically; or (2) file *Consent to Electronic Service and Notice of Electronic Service Address* (form EFS-005-CV).

The Orange County Bar Association commented that "the provision for manifesting affirmative consent should reference by definition the requirements of CCP §1010.6 for 'express consent' rather than using the phrase 'manifest affirmative consent' which is merely a subset definition in the statute[.]"

a. Subcommittee and staff review

The full requirements, not just a subset, of section 1010.6's express consent requirements are already captured in the rules. Concerning express consent, section 1010.6 states,

> Express consent to electronic service may be accomplished either by (I) serving a notice on all the parties and filing the notice with the court, or (II) manifesting affirmative consent through electronic means with the court or the court's electronic filing service provider, and concurrently providing the party's electronic address with that consent for the purpose of receiving electronic service. The act of electronic filing shall not be construed as express consent.

(§ 1010.6(a)(2)(A)(ii).) The option to serve a notice on all parties is in existing rule 2.251(b)(1)(A).

2. Responses to request for specific comments

Because there was some uncertainty on how a court or other parties would know someone had affirmatively consented to electronic service by electronic means, the invitation comment asked for specific comments on: (1) how notice is to be given to the court that a party or other person has provided express consent, or (2) how notice of the same is to be given to other parties or persons in the case. Two commenters submitted comments responsive to these questions.

The Orange County Bar Association commented, "the proposed Rule should specifically address how notice of express consent is to be given to the court and other parties and persons; since the statute is ambiguous in those regards the Council should adopt any simple notice or proof of service procedure as may be in conformity with CCP §1010.6."

The Superior Court of California, County of San Diego commented:

> Our court proposes that the committee create standard language for parties to consent to service by the method outlined in 2.251(b)(1)(C)(i). The court or court's electronic filing service providers could then include that language in their filing portal, which would allow parties to consent by accepting the terms. A copy of the acceptance would then be transmitted to the court by the service provider. If express consent is provided by filing a Consent to Electronic Service and Notice of Electronic Service Address (JC Form # EFS-005-CV) as indicated in 2.251(b)(1)(C)(ii), the court is provided notice through the filing. Our court proposes that the rule include that if a party manifests affirmative consent by either of the methods listed in 2.251(b)(1)(C), he/she is required to serve notice on all other parties.

a. Subcommittee and staff review

The provision of standard language in the rule as recommended by the Superior Court of California, County of San Diego would create uniformity statewide, which may provide more certainty that consent had been obtained as language would not potentially differ from one electronic filing service provider to the next. A transmittal of the party's acceptance of consent to the court, in the absence of filing a form, may resolve the issue of how the court can know about the consent. These topics could potentially be addressed in next year's rules cycle to refine the rule.

C. Additional comments

1. Impacts on court operations

The TCPJAC/CEAC Joint Rules Subcommittee commented on expected impacts on court operations. Specifically:

- Impact on existing automated systems (e.g., case management system, accounting system, technology infrastructure or security equipment, Jury Plus/ACS, etc.)
- Increases court staff workload.
- New configurations and workflows will have to be designed and implemented in all case management systems to manage the notices and the potential for withdrawal of consent.

a. Subcommittee and staff review

The impacts on court operations are will be included with the Judicial Council report. ITAC staff clarified with TCPJAC/CEAC Joint Rules Subcommittee staff that the concerns specifically related to rule 2.251 and that "the major issue is the creation of a system of procedures and technological changes to track consent and to handle withdrawal of consent".

2. Rule 2.251(c), mandatory electronic service

The Superior Court, County of Los Angeles submitted comments regarding rule 2.251(c)(1). Rule 2.251(c) governs electronic service required by local rule or court order and rule 2.251(c)(1) provides: "A court may require parties to serve documents electronically in specified actions by local rule or court order, as provided in Code of Civil Procedure section 1010.6 and the rules in this chapter." The court commented:

> To ensure that there is no confusion between 2.251(b) and (c). We recommend amending 2.251(c) Electronic service required by local rule or court order to read:
>
> "(1) Notwithstanding any provisions regarding consent to electronic service, a court may require parties to serve documents electronically in specified actions by local rule or court order, as provided in Code of Civil Procedure section 1010.6 and the rules in this chapter."

a. Subcommittee and staff review

This comment is out of the scope of the proposed amendments. It is a statement of existing law, but the subcommittee may consider it for clarifying purposes when reviewing material for next year's rule cycle.

Recommendations

Recommend the proposed rule amendments for Judicial Council adoption at its November 2018 meeting.

Attachments and Links

1. Text of proposed amendments to the California Rules of Court, rules 2.250, 2.251, 2.255, and 2.257, at pages 7-12.
2. Chart of comments, at pages 13-17.
3. Draft Judicial Council Report (minus attachments to the report), at pages 18-24.
4. Link A: Code of Civil Procedure section 1010.6, http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CCP§ionNum=1010.6

Rules 2.250, 2.251, 2.255, and 2.257 of the California Rules of Court would be amended, effective January 1, 2019, to read:

Rule 2.250. Construction and definitions

(a) * * *

(b) Definitions

As used in this chapter, unless the context otherwise requires:

(1) A “document” is a pleading, ~~a paper,~~ a declaration, an exhibit, or another ~~filing~~ writing submitted by a party or other person, or by an agent of a party or other person on the party’s or other person’s behalf. A document is also a notice, order, judgment, or other issuance by the court. A document may be in paper or electronic form.

(2) “Electronic service” has the same meaning as defined in Code of Civil Procedure section 1010.6 ~~is service of a document on a party or other person by either electronic transmission or electronic notification. Electronic service may be performed directly by a party or other person, by an agent of a party or other person, including the party’s or other person’s attorney, through an electronic filing service provider, or by a court~~.

(3) “Electronic transmission” has the same meaning as defined in Code of Civil Procedure section 1010.6 ~~means the transmission of a document by electronic means to the electronic service address at or through which a party or other person has authorized electronic service~~.

(4) “Electronic notification” has the same meaning as defined in Code of Civil Procedure section 1010.6 ~~means the notification of a party or other person that a document is served by sending an electronic message to the electronic service address at or through which the party or other person has authorized electronic service, specifying the exact name of the document served and providing a hyperlink at which the served document can be viewed and downloaded~~.

(5)–(8) * * *

(9) An “electronic filing manager” is a service that acts as an intermediary between a court and various electronic filing service provider solutions certified for filing into California courts.

(10) “Self-represented” means a party or other person who is unrepresented in an action by an attorney and does not include an attorney appearing in an action who represents himself or herself.

Rule 2.251. Electronic service

(a) * * *

(b) Electronic service by express consent ~~of the parties~~

(1) ~~Electronic service may be established by consent.~~ A party or other person indicates that the party or other person agrees to accept electronic service by:

(A) Serving a notice on all parties and other persons that the party or other person accepts electronic service and filing the notice with the court. The notice must include the electronic service address at which the party or other person agrees to accept service; or

(B) ~~Electronically filing any document with the court. The act of electronic filing is evidence that the party or other person agrees to accept service at the electronic service address the party or other person has furnished to the court under rule 2.256(a)(4). This subparagraph (B) does not apply to self-represented parties or other self-represented persons; they must affirmatively consent to electronic service under subparagraph (A).~~ Manifesting affirmative consent through electronic means with the court or the court's electronic filing service provider, and concurrently providing the party's electronic service address with that consent for the purpose of receiving electronic service.

(C) A party or other person may manifest affirmative consent under (B) by:

(i) Agreeing to the terms of service agreement with an electronic filing service provider, which clearly states that agreement constitutes consent to receive electronic service electronically; or

(ii) Filing *Consent to Electronic Service and Notice of Electronic Service Address* (form EFS-005-CV).

(2) A party or other person that has consented to electronic service under (1) and has used an electronic filing service provider to serve and file documents in a case consents to service on that electronic filing service provider as the designated agent for service for the party or other person in the case, until such time as the party or other person designates a different agent for service.

(c)–(k) * * *

Rule 2.255. Contracts with electronic filing service providers and electronic filing managers

(a) Right to contract

(1) A court may contract with one or more electronic filing service providers to furnish and maintain an electronic filing system for the court.

(2) If the court contracts with an electronic filing service provider, it may require electronic filers to transmit the documents to the provider.

(3) A court may contract with one or more electronic filing managers to act as an intermediary between the court and electronic filing service providers.

~~(3)~~(4) If the court contracts with an electronic service provider or the court has an in-house system, the provider or system must accept filing from other electronic filing service providers to the extent the provider or system is compatible with them.

(b) Provisions of contract

(1) The court's contract with an electronic filing service provider may:

(A) Allow the provider to charge electronic filers a reasonable fee in addition to the court's filing fee;

(B) Allow the provider to make other reasonable requirements for use of the electronic filing system.

(2) The court's contract with an electronic filing service provider must comply with the requirements of Code of Civil Procedure section 1010.6.

(3) The court's contract with an electronic filing manager must comply with the requirements of Code of Civil Procedure section 1010.6.

(c) Transmission of filing to court

(1) An electronic filing service provider must promptly transmit any electronic filing and any applicable filing fee to the court~~.~~ directly or through the court's electronic filing manager.

(2) An electronic filing manager must promptly transmit an electronic filing and any applicable filing fee to the court.

(d) Confirmation of receipt and filing of document

(1) An electronic filing service provider must promptly send to an electronic filer its confirmation of the receipt of any document that the filer has transmitted to the provider for filing with the court.

(2) The electronic filing service provider must send its confirmation to the filer's electronic service address and must indicate the date and time of receipt, in accordance with rule 2.259(a).

(3) After reviewing the documents, the court must promptly transmit to the electronic filing service provider and the electronic filer the court's confirmation of filing or notice of rejection of filing, in accordance with rule 2.259.

(e) Ownership of information

All contracts between the court and electronic filing service providers or the court and electronic filing managers must acknowledge that the court is the owner of the contents of the filing system and has the exclusive right to control the system's use.

(f) Establishing a filer account with an electronic filing service provider

(1) An electronic filing service provider may not require a filer to provide a credit card, debit card, or bank account information to create an account with the electronic filing service provider.

(2) This provision applies only to the creation of an account and not to the use of an electronic filing service provider's services. An electronic filing services provider may require a filer to provide a credit card, debit card, or bank account information before rendering services unless the services are within the scope of a fee waiver granted by the court to the filer.

Rule 2.257. Requirements for signatures on documents

(a) Electronic signature

An electronic signature is an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign a document or record created, generated, sent, communicated, received, or stored by electronic means.

~~(a)~~(b)Documents signed under penalty of perjury

When a document to be filed electronically provides for a signature under penalty of perjury of any person, the document is deemed to have been signed by that person if filed electronically provided that either of the following conditions is satisfied:

(1) The declarant has signed the document using an electronic signature ~~a computer or other technology~~, ~~in accordance with procedures, standards, and guidelines established by the Judicial Council~~ and declares under penalty of perjury under the laws of the state of California that the information submitted is true and correct; or

(2) The declarant, before filing, has physically signed a printed form of the document. By electronically filing the document, the electronic filer certifies that the original, signed document is available for inspection and copying at the request of the court or any other party. In the event this second method of submitting documents electronically under penalty of perjury is used, the following conditions apply:

(A) At any time after the electronic version of the document is filed, any party may serve a demand for production of the original signed document. The demand must be served on all other parties but need not be filed with the court.

(B) Within five days of service of the demand under (A), the party or other person on whom the demand is made must make the original signed document available for inspection and copying by all other parties.

(C) At any time after the electronic version of the document is filed, the court may order the filing party or other person to produce the original signed document in court for inspection and copying by the court. The order must specify the date, time, and place for the production and must be served on all parties.

(D) Notwithstanding (A)–(C), local child support agencies may maintain original, signed pleadings by way of an electronic copy in the statewide automated child support system and must maintain them only for the period of time stated in Government Code section 68152(a). If the local child support agency maintains an electronic copy of the original, signed pleading in the statewide automated child support system, it may destroy the paper original.

~~**(b)**~~**(c)** * * *

~~**(c)**~~**(d)** * * *

~~**(d)**~~**(e)** * * *

~~**(e)**~~**(f)** * * *

~~**Advisory Committee Comment**~~

~~**Subdivision (a)(1).** The standards and guidelines for electronic signatures that satisfy the requirements for an electronic signature under penalty of perjury are contained in the Trial Court Records Manual.~~

ITC SPR18-36
Technology: Rules Modernization Project

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

#	Commentator	Position	Comment	[**DRAFT**] Committee Response
1	1971 By Thomas S Hubbard, Jr. President & CEO Organization: 1971 311 Cobblestone Court Chapel Hill, NC 27514 Tel: 571-721-1485 Email: TSHUBBARDJR@AMVSR.COM	A	[Comments omitted. Comments were of a commercial nature unrelated to the proposal.]	The committee appreciates the support.
2	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	AM	The OCBA provides the following responses to the request for specific comments: (a) we believe the proposal appropriately addresses the stated purposes if amended as below; (b) the provision for manifesting affirmative consent should reference by definition the requirements of CCP §1010.6 for "express consent" rather than using the phrase "manifest affirmative consent" which is merely a subset definition in the statute; (c) the proposed Rule should specifically address how notice of express consent is to be given to the court and other parties and persons; since the statute is ambiguous in	The committee appreciates the support and recommendations. With respect to (b), the committee notes that the rules capture the full scope of Code of Civil Procedure section 1010.6's express consent requirements. The option to serve a notice on all parties is in existing rule 2.251(b)(1)(A).

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

ITC SPR18-36
Technology: Rules Modernization Project

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

			those regards the Council should adopt any simple notice or proof of service procedure as may be in conformity with CCP §1010.6.	
3	Superior Court of California, County of Los Angeles By Sandra Pigati-Pizano, Management Analyst Management Research Unit 111 N. Hill Street, Room 620 Los Angeles, CA 90012 Tel: 213-633-0452	AM	**Suggested Modifications:** **Rule 2.250 (b)(1)** The proposed definition allows confusion, inasmuch as it leaves open the possibility of a person e-filing a hearing exhibit, or trial exhibit. The language should explicitly exclude such exhibits from the definition in 2.250(b)(1), or allow courts to exclude them through local rules. **Rule 2.251 (c)(1)** To ensure that there is no confusion between 2.251(b) and (c). We recommend amending **2.251(c) Electronic service required by local rule or court order** to read: "(1) **Notwithstanding any provisions regarding consent to electronic service, a** court may require parties to serve documents	The committee appreciates the support and recommendations. "Exhibit" is part of the existing rule definition and not impacted by the amendment. The court does have authority to make local rules on electronic filing under rule 2.253. Rule 2.251(c)(1) is not within the scope of the proposal, but the committee appreciates that the suggested language may improve clarity. The committee may consider the recommendations for next year's rules cycle.

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

ITC SPR18-36
Technology: Rules Modernization Project

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

			electronically in specified actions by local rule or court order, as provided in Code of Civil Procedure section 1010.6 and the rules in this chapter."	
4	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. The amendments to rule 2.251(b) bring the rule into compliance with section 1010.6's express consent requirements. In addition, the rule adds a provision for how a party or other person may "manifest affirmative consent." Q: Is the provision for manifesting affirmative consent clear and does it adequately capture how a party or other person may manifest affirmative consent? Yes. Q: Rule 2.251(b) does not detail (1) how notice is to be given to the court that a party or other person has provided express consent, or (2) how notice of the same is to be given to other parties or persons in	The committee appreciates the support and recommendations. The comments are helpful in the committee's consideration of how the manifestation of affirmative consent will work and the committee may consider the recommendations to refine the rules in the next rules cycle.

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

ITC SPR18-36
Technology: Rules Modernization Project

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

			the case. The committee seeks specific comments on how such notification should be addressed in the rules. Our court proposes that the committee create standard language for parties to consent to service by the method outlined in 2.251(b)(1)(C)(i). The court or court's electronic filing service providers could then include that language in their filing portal, which would allow parties to consent by accepting the terms. A copy of the acceptance would then be transmitted to the court by the service provider. If express consent is provided by filing a Consent to Electronic Service and Notice of Electronic Service Address (JC Form # EFS-005-CV) as indicated in 2.251(b)(1)(C)(ii), the court is provided notice through the filing. Our court proposes that the rule include that if a party manifests affirmative consent by either of the methods listed in 2.251(b)(1)(C), he/she is required to serve notice on all other parties.	

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

ITC SPR18-36
Technology: Rules Modernization Project

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

5	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 JRS notes the following impact to court operations: • Impact on existing automated systems (e.g., case management system, accounting system, technology infrastructure or security equipment, Jury Plus/ACS, etc.) • Increases court staff workload. • New configurations and workflows will have to be designed and implemented in all case management systems to manage the notices and the potential for withdrawal of consent. *Suggested Modifications:* Rule 2.250 (b)(1) The proposed definition allows confusion, inasmuch as it leaves open the possibility of a person e-filing a hearing exhibit, or trial exhibit. The language should explicitly exclude such exhibits from the definition in 2.250(b)(1), or allow courts to exclude them through local rules.	The committee appreciates the support, insight into the impact on court operations, and rule recommendation. The inclusion of "exhibit" in the definition of "document" is part of the existing rule definition and not impacted by the amendment. The court does have authority to make local rules on electronic filing under rule 2.253.

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

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 20-21, 2018:

Title
Rules and Forms: Electronic Filing and Service

Rules, Forms, Standards, or Statutes Affected
Amend Cal. Rules of Court, rules 2.250, 2.251, 2.255, and 2.257

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

Agenda Item Type
Action Required

Effective Date
January 1, 2019

Date of Report
June 25, 2018

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

Executive Summary

The Information Technology Advisory Committee recommends amending several rules related to electronic service and electronic filing. The purpose of the proposal is to conform the rules to the Code of Civil Procedure, clarify and remove redundancies in rule definitions, and ensure indigent filers are not required to have a payment mechanism to create an account with electronic filing service providers.

Recommendation

The Information Technology Advisory Committee recommends, effective January 1, 2017, the Judicial Council:

1. Amend rule 2.250 to:
   - Clarify the definition of "document."
   - Revise the definitions of "electronic service," "electronic transmission," and "electronic notification" in rule 2.250(b) to refer to the definitions in section 1010.6 rather than duplicate them.
   - Add a definition of "electronic filing manager" because it is a new term used in the rules.

- Add a definition of "self-represented" which excludes attorneys rules applicable to self-represented persons were intended to add protections for persons untrained in the law, not attorneys.

2. Amend rule 2.251 to require express consent for permissive electronic service consistent with the requirements of Code of Civil Procedure section 1010.6
3. Amend rule 2.255 to:
   - Add electronic filing managers within the scope of the rule to ensure contracts with electronic filing managers will comply with Code of Civil Procedure section 1010.6.
   - Add a requirement that electronic filing service providers allow filers to create an account without having to provide payment information.
4. Amend rule 2.257 to create a procedure for electronically filed documents signed under penalty of perjury as required by Code of Civil Procedure section 1010.6.

The text of the amended rules are attached at pages X–XX [TBD when report is finalized].

Relevant Previous Council Action

In 2017, the Judicial Council sponsored Assembly Bill 976, which amended provisions of Code of Civil Procedure section 1010.6 to (1) authorize the use of electronic signatures for signatures made under penalty of perjury on electronically filed documents, (2) provide for a consistent effective date of electronic filing and service across courts and case types, (3) consolidate the mandatory electronic filing provisions, and (4) codify provisions that are currently in the California Rules of Court on mandatory electronic service, effective date of electronic service, protections for self-represented persons, and proof of electronic service. The Legislature amended AB 976 to add a provision that requires that, starting January 1, 2019, parties and other persons must provide express consent to permissive electronic service.

Analysis/Rationale

The purpose of the proposal is to conform the rules to the Code of Civil Procedure, clarify and remove redundancies in rule definitions, and ensure indigent filers are not required to have a payment mechanism to create an account with electronic filing service providers.

Amendments to rule 2.250

Rule 2.250 contains the definitions for terms used in the electronic and filing service rules found in title 2, division 3, chapter 2 of the rules of court.

Amending the definition of "document."

The current wording of the definition states that a document, in relevant part, is "a pleading, a paper, a declaration, an exhibit, or another filing…" (Cal. Rules of Court, rule 2.250(b)(1), emphasis added.) This can be read to mean that a document must be something filed with the court and thus, for example, would exclude written discovery demands and responses. The proposed amendment removes this ambiguity by striking "filing" and replacing it with "writing." In addition, the amendment strikes "a paper" from "a pleading, a paper, a declaration, an exhibit…" because it is unnecessary in the definition.

Amending the definitions of "electronic service," "electronic transmission," and "electronic notification."

The current definitions of "electronic service," "electronic transmission," and "electronic notification" in the rules duplicate Code of Civil Procedure section 1010.6's of those same terms. The amendments retain the terms in the rules' scheme of definitions, but for the actual definition components, delete the duplicative language and refer instead to Code of Civil Procedure section 1010.6. This reduces redundancies between the rules and Code of Civil Procedure and avoids the risk of the rules and Code of Civil Procedure differing in their definitions should the Legislature amend Code of Civil Procedure section 1010.6.

Adding a definition of "electronic filing manager."

The proposal includes amendments to rule 2.255, which add electronic filing managers within the scope of the rule. Because the term "electronic filing manager" was not previously used in the electronic filing and service rules, it is necessary to define it. The definition is based descriptions of electronic filing managers the Judicial Council has used in past procurements for electronic filing manager contractors.

Adding a definition of "self-represented."

The proposal adds a definition for "self-represented," which excludes attorneys from the scope of the definition. Rules applicable to self-represented persons were intended to add protections for those without an attorney. For example, self-represented persons are exempt from mandatory electronic filing. Attorneys acting for themselves are not acting without an attorney. Accordingly, attorneys are excluded from the definition of "self-represented" under the electronic filing and service rules. Because section 1010.6 uses the term "unrepresented" and the rules of court use the term "self-represented," the definition in the rules refers to self-represented parties or other persons as being those unrepresented by an attorney.

Amendments to rule 2.251

Rule 2.251 governs electronic service. The proposal amends rule 2.251(b), which governs permissive electronic service, to require express consent to electronic service and add a provision for how a party or other person may manifest consent. The current rules allow the act of electronic filing to serve as consent to electronic service. Effective January 1, 2019, Code of Civil Procedure section 1010.6 will no longer allow the act of electronic filing alone to serve as consent. (§ 1010.6(a)(2)(A)(ii).) Under section 1010.6, parties may still consent through electronic means by "manifesting affirmative consent through electronic means with the court or the court's electronic filing service provider, and concurrently providing the party's electronic service address with that consent for the purpose of receiving electronic service." The proposal amends the rules to remove the provision allowing the act of filing to serve as consent to electronic service and replaces it with the language for manifesting affirmative consent by electronic means from section 1010.6. The proposal also adds a provision for how a party or other person may "manifest affirmative consent" by agreeing to consent in an electronic service provider's terms of service or filing a form consenting to electronic service.

Amendments to rule 2.255

Rule 2.255 governs contracts with electronic filing service providers. The proposed amendments to rule 2.255 add electronic filing managers within the scope of the rule to ensure contracts with electronic filing managers will comply with Code of Civil Procedure section 1010.6, and add a requirement that electronic filing service providers allow filers to create an account without having to provide financial account information.

Adding electronic filing managers to the scope of the rule

The proposal adds electronic filing managers within the scope of rule 2.255. Code of Civil Procedure section 1010.6(g)(2) requires that "[a]ny system for the electronic filing and service of documents, including any information technology applications, Internet Web sites, and Web-based applications, used by an electronic service provider or any other vendor or contractor that provides an electronic filing and service system to a trial court" be accessible by persons with disabilities and comply with certain access standards. Vendors and contractors must comply as soon as practicable, but no later than June 30, 2019. (Code Civ. Proc, § 1010.6(g)(3).) Likewise, the statute requires the Judicial Council to adopt rules to implement the requirements as soon as practicable, but no later than June 30, 2019. (Code Civ. Proc, § 1010.6(g)(1).) Code of Civil Procedure section 1010.6 includes specific requirements that courts and contractors must meet. Rule 2.255 already requires courts' contracts with electronic filing service providers to comply with requirements of Code of Civil Procedure section 1010.6. However, because courts may also contract with electronic filing managers and the rules of court do not account for contracts with electronic filing managers, the proposal amends rule 2.255 to include them.

Adding a requirement that electronic service providers allow filers to create an account without providing payment information

The proposal amends rule 2.255 to add subdivision (f) to require electronic filing service providers to allow filers to create an account without having to provide a credit card, debit card, or bank account information. The amendment is based on a suggestion from the State Bar's Standing Committee on the Delivery of Legal Services. According to the standing committee, some electronic filing service providers require such payment information even if the filer is never charged. According to the standing committee, this "creates an insurmountable barrier to those without access to credit or banking services." Subdivision (f) provides that it only applies to the creation of an account, but not to the provision of services unless the filer has a fee waiver.

Amendments to rule 2.257

The proposal amends 2.257 to create a procedure for electronically filed documents signed under penalty of perjury. Cod of Civil Procedure section 1010.6(b)(2)(B)(ii) provides that when a document to be filed requires a signature made under penalty of perjury, the document is considered signed by the person if, in relevant part, "[t]he person has signed the document using a computer or other technology pursuant to the procedure set forth in a rule of court adopted by the Judicial Council by January 1, 2019." Accordingly, the proposal creates a procedure where the document is deemed signed when the "declarant has signed the document using an electronic signature, and declares under penalty of perjury under the laws of the state of California that the

information submitted is true and correct." The language is modeled after the requirements in the Uniform Electronic Transactions Act for electronic signatures made under penalty of perjury. (Civ. Code, § 1633.11(b).) In addition, the amendments add a definition of "electronic signature" to the rule, modeled after the definitions used in the Uniform Electronic Transactions Act and the Code of Civil Procedure.

Policy implications

The statutory requirement for the manifestation of affirmative consent through electronic means is new. The rule provisions addressing manifesting affirmative consent may require refinement in the future to address issues that may arise and become known when the requirement goes into effect on January 1, 2019.

Comments

Comments on the manifestation of affirmative consent to permissive electronic service

The Orange County Bar Association commented that "the provision for manifesting affirmative consent should reference by definition the requirements of [Code of Civil Procedure section] 1010.6 for 'express consent' rather than using the phrase 'manifest affirmative consent' which is merely a subset definition in the statute[.]"

The committee noted that the full requirements, not just a subset, of Code of Civil Procedure section 1010.6's express consent requirements are already captured in the rules. The option other than manifesting affirmative consent is to serve a notice on all the parties and filing the notice with the court." (Code Civ. Proc. § 1010.6(a)(2)(A)(ii).) This option is accounted for in existing rule 2.251(b)(1)(A).

Comments responsive to the invitation to comments' request for specific comments

Because there was some uncertainty on how a court or other parties would know someone had affirmatively consented to electronic service by electronic means, the invitation comment asked for specific comments on: (1) how notice is to be given to the court that a party or other person has provided express consent, or (2) how notice of the same is to be given to other parties or persons in the case. Two commenters submitted comments responsive to these questions recommending that the rules address how notice be given. The Superior Court of California, County of San Diego provided specific recommendations on when a party manifests consent by agreeing to consent in the terms of service with an electronic service provider. The first recommendation is that there should be standard language used for parties to consent to electronic service, and the second was that a copy of the parties' acceptance be transmitted to the court by the electronic filing service provider. The court also commented that the party consenting should serve notice on all other parties. These comments are helpful for refinement of the rules to provide greater clarity and guidance and the committee may develop them into proposals in the next rule cycle.

Alternatives considered

Amendments to rule 2.250

- The committee did not consider the alternative of not amending the definition of "document" because the existing definition contains ambiguity that may cause confusion.
- The committee considered the alternative of not amending the definitions of "electronic service," "electronic transmission," and "electronic notification." The committee received specific comments concerning this topic during the amendments to the electronic filing and service rules in 2017 and agreed with the comments that duplicating the definitions already contained in statute was unnecessary.
- The committee did not consider the alternative of not defining "electronic filing manager" because the term could be unclear if undefined.
- The committee considered the alternative of not adding a definition for "self-represented" as it has not been necessary to define it previously. However, including the definition provides greater clarity on the purpose of having separate requirements for "self-represented," which is to protect persons who do not have or who are not attorneys.

Amendments to rule 2.251

The committee considered making a technical amendment to the consent requirements in rule 2.251(b) to ensure the rules comply with Code of Civil Procedure section 1010.6's express consent requirements without interpreting the statute's requirement for "manifesting consent through electronic means." However, during the development of the proposal, the committee received public comments from the electronic filing service provider community raising concerns over uncertainty in the meaning of "manifesting affirmative consent" and providing an interpretation, which was integrated into the proposal.

Amendments to rule 2.255

The committee did not consider the alternative of not adding electronic filing managers to the scope of the rule because including electronic filing managers is necessary to comply with the requirements of Code of Civil Procedure section 10106.(g).

The court did not consider the alternative of not adding new subdivision (f) because adding the subdivision removes a barrier to filers without access to credit or banking services. The committee limited the scope of the rule to ensure it was targeted at only the ability to create an account, not to utilize the services, which can require payment information or, if applicable, a fee waiver.

Amendments to rule 2.257

The committee did not consider the alternative of not creating a procedure for electronic signatures on documents filed under penalty of perjury. Code of Civil Procedure section 1010 requires creation of the rule by January 1, 2019.

Fiscal and Operational Impacts

The Joint Rules Subcommittee of Trial Court Presiding Judges Advisory Committee and Court Executives Advisory Committees commented on expected impacts on court operations as a result of rule 2.251. Specifically:

- Impact on existing automated systems (e.g., case management system, accounting system, technology infrastructure or security equipment, Jury Plus/ACS, etc.)
- Increases court staff workload.
- New configurations and workflows will have to be designed and implemented in all case management systems to manage the notices and the potential for withdrawal of consent.

Attachments and Links

1. Text of proposed amendments to the California Rules of Court, rules 2.250, 2.251, 2.255, and 2.257, at pages XX-XX [TBD when report finalized]
2. Chart of comments, at pages XX-XX [TBD when report finalized]
3. Link A: Code of Civil Procedure section 1010.6, *http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CCP§ionNum=1010.6*

JUDICIAL COUNCIL OF CALIFORNIA

455 Golden Gate Avenue • San Francisco, California 94102-3688
Telephone 415-865-4200 • Fax 415-865-4205 • TDD 415-865-4272

MEMORANDUM

Date
June 22, 2018

To
Information Technology Advisory Committee,
Hon. Sheila F. Hanson, Chair

From
Andrea L. Jaramillo, Attorney
Legal Services, Judicial Council

Subject
Rules and Forms: Form for Withdrawal of Consent to Electronic Service

Action Requested
Please review

Deadline
July 2, 2018

Contact
Andrea L. Jaramillo
916-263-0991 phone
andrea.logue@gmail.com

Susan R. McMullan
415-865-7990 phone
susan.mcmullan@jud.ca.gov

Background

This spring, the Information Technology Advisory Committee (ITAC) and Civil and Small Claims Advisory Committee (CSCAC) circulated a form proposal for public comment. The proposed form, EFS-006, *Withdrawal of Consent to Electronic Service*, will be a new form. The purpose of the proposal is to comply with Code of Civil Procedure section 1010.6(a)(6), which requires the Judicial Council to create such a form by January 1, 2019.

On June 18, 2018, the CSCAC Rules and Forms Subcommittee recommended the form as modified by adding a notice under the title of the form that states: "This form may not be used for electronic service required by local rule or court order." On June 21, 2018, the ITAC Rules and Policy Subcommittee also recommended adding the notice with a minor addition to include the term "mandatory" before "electronic service." Both subcommittees expressed concern with Code of Civil Procedure section 1010.6(a)(6)'s provision that states, "A party or other person

who has provided express consent to accept service electronically may withdraw consent *at any time by completinsg and filing with the court* the appropriate Judicial Council form." The subcommittees were concerned that this could lead to gamesmanship with a party dropping consent around key deadlines and the other party not having sufficient notice.

Discussion

Four commenters responded to the invitation to comment either agreeing with the proposal or agreeing as modified. Three of the commenters responded to the invitation to comment's request for specific comments.

A. Add language clarifying use of the form for permissive electronic service only

The Superior Court of California, County of Los Angeles suggested that EFS-006 be modified to add the following under the title: "(This form may not be used for electronic service required by local rule or court order.)" The CSCAC Rules and Forms Subcommittee recommended that this modification be incorporated into EFS-006 and the ITAC Rules and Policy Subcommittee recommended the same with the minor addition of the word "mandatory" in the notice so that it states: "This form may not be used for mandatory electronic service required by local rule or court order." Form EFS-006 is applicable only to permissive electronic service and not mandatory electronic service, and accordingly, the notice adds clarity on the proper use of the form.

B. Responses to the request for specific comments

Three of the commenters responded to the invitation to comment's request for specific comments. The invitation to comment requested specific comments on the following questions:

- Proposed form EFS-006 includes a proof of electronic service on page 2 of the form. There is a separate proof of electronic service form, POS-050/EFS-050, available as well. In light of the availability of POS-050/EFS-050, is it necessary to include a proof of electronic service as part of EFS-006?
    - If not, should language be included on EFS-006 directing the completion of a proof of service. For example, "You must complete a proof of service for this form. You may use a Judicial Council form for the proof of service. If you electronically serve the form, you may use form POS-050/EFS-050. If you serve by mail, you may use form POS-030."

The Superior Court of California, County of Ventura commented, "It is not necessary to include a proof of electronic service as part of EFS-006 and is not helpful if limited to service by

electronic service." The court recommended the form be modified accordingly and that the example language regarding proof of service included in the second bullet point, above, be added to the form.

The Superior Courts of California, Counties of Los Angeles and San Diego both recommended that the proof of electronic service be retained on page 2 of the form. The Los Angeles court commented, "The proof of electronic service should be included on page two of EFS-006. It is useful to the filer and consistent with form EFS-005-CV." The San Diego court commented, "Since this form is likely to be used more often by self-represented litigants, it seems beneficial to include the [proof of service] and more convenient for the litigant." The San Diego court also commented that if the decision is to remove the proof of service, the proposed language for directing the completion of a proof of service is appropriate and clear.

The CSCAC Rules and Forms Subcommittee and ITAC Rules and Policy Subcommittee recommended the proof of electronic service be kept with form EFS-006. The proof of electronic service includes a note at the top that form POS-030, *Proof of Service by First–Class Mail–Civil*, should be used if service is by mail. The Superior Court of California, County of San Diego makes a good point that it is more convenient for self-represented litigants if the proof of service is included. While some litigants may elect to use form POS-030, *Proof of Service by First–Class Mail–Civil*, instead of the proof of electronic service included with form EFS-006, and, thus, have to look up an additional form, removing the proof of electronic service from form EFS-006 would require *all* litigants to look up a separate proof of service form.

Recommendations

Modify the proposed form EFS-006, *Withdrawal of Consent to Electronic Service*, to include a notice that the form may not be used for mandatory electronic service required by local rule or court order. As modified, recommend the form for Judicial Council adoption at its September 2018 meeting.

Attachments and Links

1. Form EFS-006, *Withdrawal of Consent to Electronic Service*, at pages 4-5.
2. Chart of comments, at pages 8-10.
3. Draft Judicial Council Report (minus attachments to the report), at pages 11-14.
4. Link A: Code of Civil Procedure section 1010.6, http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CCP§ionNum=1010.6

EFS-006

ATTORNEY OR PARTY WITHOUT ATTORNEY	STATE BAR NUMBER:	FOR COURT USE ONLY
NAME:		**DRAFT Not approved by the Judicial Council 2018-06-12**
FIRM NAME:		
STREET ADDRESS:		
CITY:	STATE: ZIP CODE:	
TELEPHONE NO.:	FAX NO.:	
E-MAIL ADDRESS:		
ATTORNEY FOR (*name*):		
SUPERIOR COURT OF CALIFORNIA, COUNTY OF		
STREET ADDRESS:		
MAILING ADDRESS:		
CITY AND ZIP CODE:		
BRANCH NAME:		CASE NUMBER:
PLAINTIFF/PETITIONER:		JUDICIAL OFFICER:
DEFENDANT/RESPONDENT:		
WITHDRAWAL OF CONSENT TO ELECTRONIC SERVICE		DEPARTMENT:

Notice: This form may not be used for mandatory electronic service required by local rule or court order.

1. ☐ The following self-represented party or ☐ the attorney for:

   a. ☐ plaintiff *(name):*

   b. ☐ defendant *(name):*

   c. ☐ petitioner *(name):*

   d. ☐ respondent *(name):*

   e. ☐ other *(describe and name):*

   withdraws consent to electronic service of notices and documents in the above-captioned action.

2. The mailing address for service on the person identified in item 1 is *(specify):*

   Street:

   City:

   State: Zip:

3. All notices and documents in the above-captioned action must be served on the person identified in item 1 at the address in item 2 as of *(date):*

Date:

(TYPE OR PRINT NAME) ▶ (SIGNATURE OF PARTY OR ATTORNEY)

WITHDRAWAL OF CONSENT TO ELECTRONIC SERVICE
(Electronic Filing and Service)

PLAINTIFF/PETITIONER: DEFENDANT/RESPONDENT:	CASE NUMBER:

(Note: *If you serve* Withdrawal of Consent to Electronic Service *by mail, you should use form POS-030,* Proof of Service by First-Class Mail–Civil, *instead of using this page.)*

PROOF OF ELECTRONIC SERVICE

WITHDRAWAL OF CONSENT TO ELECTRONIC SERVICE

1. I am at least 18 years old.

   My residence or business address is *(specify):*

2. I electronically served a copy of the *Withdrawal of Consent to Electronic Service* as follows:

   a. Name of person served:

      On behalf of *(name or names of parties represented, if person served is an attorney):*

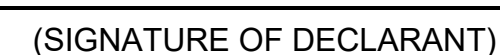
   b. Electronic service address of person served:

   c. On *(date):*

☐ Electronic service of the *Withdrawal of Consent to Electronic Service* on additional persons is described in an attachment.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Date:



(TYPE OR PRINT NAME OF DECLARANT) ▶ (SIGNATURE OF DECLARANT)

ITC SPR18-38
Technology: Rules Modernization Project Proposed Rules

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

#	Commentator	Position	Comment	[**DRAFT**] Committee Response
1	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	A	No specific comment.	The committees appreciate the support.
2	Superior Court of California, County of Los Angeles By Sandra Pigati-Pizano, Management Analyst Management Research Unit 111 N. Hill Street, Room 620 Los Angeles, CA 90012 Tel: 213-633-0452	AM	Suggested Modification: Form EFS-006 Under the title: Withdrawal of Consent to Electronic Service add: (This form may not be used for electronic service required by local rule or court order.) Request for Specific Comments: Proposed form EFS-006 includes a proof of electronic service on page 2 of the form. There is a separate proof of electronic service form, POS-050/EFS-050, available as well. In light of the availability of POS-050/EFS-050, is it necessary to include	The committees appreciate the support, suggested modification, and responses to the request for specific comments. The suggested modification adds clarity to the form and the committee will recommend it with a minor addition of the word "mandatory" before "electronic service."

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

ITC SPR18-38
Technology: Rules Modernization Project Proposed Rules

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

#	Commentator	Position	Comment	[DRAFT] Committee Response
			a proof of electronic service as part of EFS-006? The proof of electronic service should be included on page two of EFS-006. It is useful to the filer and consistent with form EFS-005-CV.	
3	Superior Court of California, County of San Diego By Mike Roddy, Executive Officer 1100 Union Street San Diego, CA 92101	A	Q: Proposed form EFS-006 includes a proof of electronic service on page 2 of the form. There is a separate proof of electronic service form, POS-050/EFS-050, available as well. In light of the availability of POS-050/EFS-050, is it necessary to include a proof of electronic service as part of EFS-006? Since this form is likely to be used more often by self-represented litigants, it seems beneficial to include the POS and more convenient for the litigant. Q If not, should language be included on EFS-006 directing the completion of a proof of	The committees appreciate the support and responses to the request for specific comments.

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

ITC SPR18-38
Technology: Rules Modernization Project Proposed Rules

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

#	Commentator	Position	Comment	[**DRAFT**] Committee Response
			service. For example, "You must complete a proof of service for this form. You may use a Judicial Council form for the proof of service. If you electronically serve the form, you may use form POS-050/EFS-050. If you serve by mail, you may use form POS-030." If the committee elects to remove the POS on page two, then the proposed language is appropriate and clear.	
4	Superior Court of California, County of Ventura By Julie Camacho, Court Manager 800 S. Victoria Avenue Ventura CA, 93006 Email: julie.camacho@ventura.courts.ca.gov	AM	It is not necessary to include a proof of electronic service as part of EFS-006 and is not helpful if limited to service by electronic service. Yes, the indicated language regarding proof of service should be added to the form.	The committees appreciate the support and responses to the request for specific comments.

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

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 20-21, 2018:

Title
Rules and Forms: Form for Withdrawal of Consent to Electronic Service

Rules, Forms, Standards, or Statutes Affected
Adopt form EFS-006, *Withdrawal of Consent to Electronic Service*

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

Civil and Small Claims Advisory Committee
Hon. Ann I. Jones, Chair

Agenda Item Type
Action Required

Effective Date
January 1, 2019

Date of Report
June 22, 2018

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

Anne Ronan, 415-865-8933
anne.ronan@jud.ca.gov

Executive Summary

The Information Technology Advisory Committee and Civil and Small Claims Advisory Committee recommend the Judicial Council adopt a new form for withdrawal of consent to electronic service. The purpose of the proposal is to comply with Code of Civil Procedure section 1010.6(a)(6), which requires the Judicial Council to create such a form by January 1, 2019.

Recommendation

The Information Technology Advisory Committee and Civil and Small Claims Advisory Committee recommend the Judicial Council adopt form EFS-006, *Withdrawal of Consent to Electronic Service*, effective January 1, 2019. The text of the new form is attached at pages [X–XX, TBD when report is finalized].

Relevant Previous Council Action

In 2017, the Judicial Council sponsored Assembly Bill 976, which amended provisions of Code of Civil Procedure section 1010.6 to (1) authorize the use of electronic signatures for signatures made under penalty of perjury on electronically filed documents, (2) provide for a consistent effective date of electronic filing and service across courts and case types, (3) consolidate the mandatory electronic filing provisions, and (4) codify provisions that are currently in the California Rules of Court on mandatory electronic service, effective date of electronic service, protections for self-represented persons, and proof of electronic service. The Legislature amended AB 976 to add a provision that requires the Judicial Council to create, by January 1, 2019, a form for a party or other person to withdraw their consent to permissive electronic service.

Analysis/Rationale

Code of Civil Procedure section 1010.6(a)(6) requires the Judicial Council to create a form for withdrawal of consent to electronic service by January 1, 2019. For the sake of consistency, the recommended form, EFS-006, *Withdrawal of Consent to Electronic Service*, is modeled after existing form EFS-005-CV, *Consent to Electronic Service and Notice of Electronic Service Address.*

Policy implications

The proposed form does not have significant policy implications. The form merely creates a formal mechanism for parties to use to withdraw consent to permissive electronic service.

Comments

Four commenters responded to the invitation to comment either agreeing with the proposal or agreeing as modified. Three of the commenters responded to the invitation to comment's request for specific comments.

Add language clarifying use of the form for permissive electronic service only

The Superior Court of California, County of Los Angeles suggested that EFS-006 be modified to add the following under the title: "(This form may not be used for electronic service required by local rule or court order.)" The committees decided to incorporate the modification into EFS-006 with the addition of the word "mandatory" between "used for" and "electronic service" so the notice states, "This form may not be used for mandatory electronic service required by local rule or court order." The form is applicable only to permissive electronic service and not mandatory electronic service. Accordingly, the modification adds clarity on the proper use of the form.

Commented [JA1]: TBD, may be revised and will be finalized following committee meetings

Commented [JA2]: TBD, the rationale may be revised and will be finalized following the committee meetings

Responses to the request for specific comments

Three of the commenters responded to the invitation to comment's request for specific comments. The invitation to comment requested specific comments on the following questions:

DRAFT

- Proposed form EFS-006 includes a proof of electronic service on page 2 of the form. There is a separate proof of electronic service form, POS-050/EFS-050, available as well. In light of the availability of POS-050/EFS-050, is it necessary to include a proof of electronic service as part of EFS-006?
    - If not, should language be included on EFS-006 directing the completion of a proof of service. For example, "You must complete a proof of service for this form. You may use a Judicial Council form for the proof of service. If you electronically serve the form, you may use form POS-050/EFS-050. If you serve by mail, you may use form POS-030."

The Superior Court of California, County of Ventura commented, "It is not necessary to include a proof of electronic service as part of EFS-006 and is not helpful if limited to service by electronic service." The court recommended the form be modified accordingly and that the example language regarding proof of service included in the second bullet point, above, be added to the form.

The Superior Courts of California, Counties of Los Angeles and San Diego both recommended that the proof of electronic service be retained on page 2 of the form. The Los Angeles court commented, "The proof of electronic service should be included on page two of EFS-006. It is useful to the filer and consistent with form EFS-005-CV." The San Diego court commented, "Since this form is likely to be used more often by self-represented litigants, it seems beneficial to include the [proof of service] and more convenient for the litigant." The San Diego court also commented that if the decision is to remove the proof of service, the proposed language for directing the completion of a proof of service is appropriate and clear.

The committees decided the proof of electronic service would be kept with form EFS-006 because it is more convenient for litigants for the proof of service to be included. While some litigants may elect to use form POS-030, *Proof of Service by First–Class Mail–Civil*, instead of the proof of electronic service included with form EFS-006, and, thus, have to look up an additional form, removing the proof of electronic service from form EFS-006 would require *all* litigants to look up a separate proof of service form.

Commented [JA3]: TBD, this may be revised and will be finalized following the committee meetings

Commented [JA4]: TBD, the reasons may be revised and will be finalized following the committee meetings

Internal comments concerning the ability to withdraw consent at any time by filing a form with the court

Both committees expressed concern with Code of Civil Procedure section 1010.6(a)(6)'s provision that states, "A party or other person who has provided express consent to accept service electronically may withdraw consent *at any time by completing and filing with the court* the appropriate Judicial Council form." The committees were concerned that this could lead to gamesmanship with a party dropping consent around key deadlines and the other party not having sufficient notice. This may require a legislative proposal in the future.

DRAFT

Alternatives considered

The committees did not consider the alternative of not creating EFS-006, *Withdrawal of Consent to Electronic Service*, because statute mandates the creation of the form.

Fiscal and Operational Impacts

It is not expected that the new form will result in any significant costs or operational impacts on the courts.

Attachments and Links

1. Form EFS-006, *Withdrawal of Consent to Electronic Service*, at pages XX-XX, TBD
2. Chart of comments, at pages XX–XX, TBD
3. Link A: Code of Civil Procedure section 1010.6, *http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CCP§ionNum=1010.6*

DRAFT

JUDICIAL COUNCIL OF CALIFORNIA

455 Golden Gate Avenue • San Francisco, California 94102-3688
Telephone 415-865-4200 • Fax 415-865-4205 • TDD 415-865-4272

MEMORANDUM

Date
June 26, 2018

To
Information Technology Advisory Committee
Hon. Sheila F. Hanson, Chair

From
Andrea L. Jaramillo, Attorney
Legal Services

Subject
Rules Proposal: Review public comments and make recommendation on adopting Cal. Rules of Court, rules 2.515–2.528 and 2.540–2.545; amending rules 2.500–2.503

Action Requested
Please review

Deadline
July 2, 2018

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

Background

This spring, the Information Technology Advisory Committee (ITAC) circulated a rules proposal for public comment that would proposal make limited amendments to rules governing public access to electronic trial court records and create a new set of rules governing remote access to such records by parties, parties' attorneys, court-appointed persons, legal organizations, qualified legal services projects, and government entities. The purpose of the proposal is to facilitate existing relationships and provide clear authority to the courts. The public comment period ended on June 8, 2018. The Joint Ad Hoc Subcommittee on Remote Access met on June 22, 2018 to consider public comments and recommended modifications to the proposed rules based on the public comments and subcommittee members' discussion.

Discussion

Thirteen commenters submitted comments in response to the invitation to comment. Given the volume of information, to facilitate the committee's discussion and review of the comments, the attached materials include the proposed rules and amendments with drafter's notes immediately following each proposal that received public comment. The drafter's notes list the specific comments received in response to the proposal, and are followed by subcommittee and staff review and recommendations.

The drafter's notes are organized as follows:

- Comments that pertained to specific rule appear directly after that rule so they may be viewed in context. For example, comments on rule 2.518 appear directly after rule 2.518.
- Comments responsive to the request for specific comments that are not tied to a particular rule appear at the end of the proposed rules.
- Comments that do not pertain to a specific rule or request for specific comments appear after the comments responsive to the request for specific comments under "Other Comments."

For purposes of ITAC's meeting on July 2, 2018, the subcommittee chair and staff will focus the ITAC discussion on the topics that generated the most interest and reserve time at the end for any additional items ITAC members may want to discuss. The topics that generated the most interest in the proposal include:

- 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 (rule 2.526).
- Provisions for remote access by Department of Child Support Services and local child support agencies (rule 2.540).

Recommendations

Recommend the proposed rules and rule amendments, as modified by subcommittee and staff recommendations, for Judicial Council adoption at its November 2018 meeting.

Attachments and Links

1. Text of proposed adoption of the California Rules of Court, rules 2.515–2.528 and 2.540–2.545; and proposed amendments to rules 2.500–2.503, at pages 4-60.
2. Chart of comments, at pages 61-113.
3. Draft Judicial Council Report (minus attachments to the report), at pages **TBD**. (The Judicial Council report is still being drafted and will be distributed in an update to the ITAC meeting materials.)
4. Link A: California 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 2.515–2.528 and 2.540–2.545 of the California Rules of Court are adopted and rules 2.500–2.503 are amended, effective January 1, 2019, to read:

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

<u>Article 1. General Provisions</u>

Rule 2.500. Statement of purpose

(a) Intent

The rules in this chapter are intended to provide the public<u>, parties, parties' attorneys, legal organizations, court-appointed persons, and government entities</u> 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<u>,</u> ~~and~~ the public<u>, parties, parties' attorneys, legal organizations, court-appointed persons, and government entities</u> 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<u>, parties, parties' attorneys, legal organizations, court-appointed persons, and government entities</u> 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 <u>is</u> gained from the experience of ~~the courts in~~ providing electronic access under these rules.

DRAFT

1
2 **Rule 2.501. Application, ~~and~~ scope, and information to the public**
3
4 **(a) Application and scope**
5
6 The rules in this chapter apply only to trial court records as defined in rule
7 2.502(4). They do not apply to statutorily mandated reporting between or within
8 government entities, or any other documents or materials that are not court records.
9
10 **(b) ~~Access by parties and attorneys~~ Information to the public**
11
12 ~~The rules in this chapter apply only to access to court records by the public. They~~
13 ~~do not limit access to court records by a party to an action or proceeding, by the~~
14 ~~attorney of a party, or by other persons or entities that are entitled to access by~~
15 ~~statute or rule.~~
16
17 The websites for all trial courts must include a link to information that will inform
18 the public of who may access their electronic records under the rules in this chapter
19 and under what conditions they may do so. This information will be posted publicly
20 on *www.courts.ca.gov*. Each trial court may post additional information, in plain
21 language, as necessary to inform the public about the level of access that the
22 particular trial court is providing.
23
24 ***Drafter's Note:*** The following comment was received in response to the
25 proposed amendment of rule 2.501(b):
26
27 • Orange County Bar Association. Rule 2.501(b) appears to grant individed
28 trial courts rights to further define and limit access which defeats the very
29 purpose of these proposed "uniform" rules.
30
31 ***Subcommittee and staff review:*** Rule 2.501(b) only addresses providing plain
32 language information to the public about access to electronic records. The new
33 provisions governing remote access in article 3 and 4 provide for authority and
34 responsibility of the courts. Those provisions broaden the opportunities to provide
35 remote access and do not limit the existing public access rules.
36
37 **Advisory Committee Comment**
38
39 The rules on remote access do not apply beyond court records to other types of documents,
40 information, or data. Rule 2.502 defines a court record as "any document, paper, or exhibit filed
41 in an action or proceeding; any order or judgment of the court; and any item listed in Government
42 Code section 68151(a), excluding any reporter's transcript for which the reporter is entitled to
43 receive a fee for any copy. The term does not include the personal notes or preliminary

1 memoranda of judges or other judicial branch personnel, statutorily mandated reporting between
2 government entities, judicial administrative records, court case information, or compilations of
3 data drawn from court records where the compilations are not themselves contained in a court
4 record." (Rule 2.502(4), Cal. Rules of Court.) Thus, courts generate and maintain many types of
5 information that are not court records and to which access may be restricted by law. Such
6 information is not remotely accessible as court records, even to parties and their attorneys. If
7 parties and their attorneys are entitled to access to any such additional information, separate and
8 independent grounds for that access must exist.
9
10 **Rule 2.502. Definitions**
11
12 As used in this chapter, the following definitions apply:
13
14 (1) "Authorized person" means a person authorized by a legal organization, qualified
15 legal services project, or government entity to access electronic records.
16
17 (2) "Brief legal services" means legal assistance provided without, or before, becoming
18 a party's attorney. It includes giving advice, having a consultation, performing
19 research, investigating case facts, drafting documents, and making limited third-
20 party contacts on behalf of a client.
21
22 ***DRAFTER'S NOTE:*** The following comments were received in response to a
23 request for specific comments on the term "brief legal services." The request for
24 specific comments asked:
25
26 The term "brief legal services" is used in the proposed rules in the context
27 of staff and volunteers of "qualified legal services organizations" providing
28 legal assistance to a client without becoming the client's attorney. The rule
29 was developed to facilitate legal aid organizations providing short-term
30 services without becoming the client's representative in a court matter. Is
31 the term "brief legal services" and its definition clear? Would an alternative
32 term like "preliminary legal services" be more clear?
33
34 • Superior Court of California, County of Orange. *Specifically in response to*
35 *"Would an alternative term like 'preliminary legal services' be more clear?*
36
37 Yes. Is the intention to allow attorneys on a case to have permanent
38 access or is there an expectation the court must manage limited-time
39 access to those that are given consent? Similar to restricted access for
40 designees. Additionally, once consent is given by a party for others to
41 have access do you intend to create a process for them to retract
42 consent?
43

Subcommittee and staff review: 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.

- Superior Court of California, County of San Diego. The proposed "brief legal services" is clear and preferred over "preliminary legal services." Preliminary makes it sound like it would only be during the case initiation phase, when in reality they could obtain assistance throughout the life of a case.

Subcommittee and staff review: The court is correct that brief legal services could occur at any time during the case.

- Superior Court of California, County of San Joaquin. Yes, it is [clear].

  On whether "preliminary legal services" should be used instead, the court commented, "No, I think it would be more confusing. 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.

Subcommittee and staff review: The subcommittee considered the comments on "brief legal services" versus "preliminary legal services" and found that "brief legal services" is the clearer term because the services could occur at any stage in a case.

~~(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.

1 (4) "Court case information" consists of information created and maintained by a court
2 about a case or cases and not part of the court records that are filed with the court.
3 This includes information in the case management system and case histories.
4
5 ***DRAFTER'S NOTE:*** The following comments was received in response to the
6 proposed adoption of rule 2.502(a)(4):
7
8 - Joint Technology Subcommittee of the Trial Court Presiding Judges and
9 Court Executives Advisory Committees, and the Superior Court of
10 California, County of Placer. Modify the definition of "court case
11 information" to use more natural language to reduce confusion. A
12 possible definition might be:
13
14 "Court case information" refers to data that is stored in a court's case
15 management system or case histories. This data supports the court's
16 management or tracking of the action and is not part of the official
17 court record for the case or cases.
18
19 ***Subcommittee and staff review:*** The proposed modification is substantively the
20 same, but more clearly written than the original draft. Accordingly, the
21 subcommittee recommends that the definition be revised to reflect the
22 commenters' wording:
23
24 (4) "Court case information" refers to data that is stored in a court's case
25 management system or case histories. This data supports the court's
26 management or tracking of the action and is not part of the official court
27 record for the case or cases.
28
29 ~~(4)~~(5) "Electronic access" means ~~computer~~ access by electronic means to court records
30 available ~~to the public~~ through ~~both~~ public terminals at the courthouse and
31 remotely, unless otherwise specified in the rules in this chapter.
32
33 ~~(2)~~(6) "Electronic record" is a ~~computerized~~ court record~~, regardless of the manner in~~
34 ~~which it has been computerized~~ that requires the use of an electronic device to
35 access. The term includes both a ~~document~~ record that has been filed electronically
36 and an electronic copy or version of a record that was filed in paper form. The term
37 does not include a court record that is maintained only on microfiche, paper, or any
38 other medium that can be read without the use of an electronic device.
39
40 (7) "Government entity" means a legal entity organized to carry on some function of
41 the State of California or a political subdivision of the State of California. A
42 government entity is also a federally recognized Indian tribe or a reservation,
43 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.

Drafter's Note: The following comments were received in response to a request for specific comments on the term "legal organization." The request for specific comments asked, "Is the term 'legal organization' and its definition clear or necessary?"

- Superior Court of California, County of Orange. Yes, it is clear and necessary.
- Superior Court of California, County of San Diego. The proposed "legal organization" is clear.
- Superior Court of California, County of San Joaquin. 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.

Subcommittee and staff review: The term "legal organization" will be retained.

(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 6213(a) of the Business and Professions Code.

(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) * * *

(2) All records in civil cases, except those listed in (c)(1)–~~(9)~~(10).

DRAFTER'S NOTE: The following comment was received in response to the proposed adoption of rule 2.503(b)(2):

- Joint Technology Subcommittee of the Trial Court Presiding Judges and Court Executives Advisory Committees, and the Superior Court of California, County of Placer. "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."

***Subcommittee and staff review**:* The subcommittee agrees. This is part of an existing rule and would be a technical correction as the case records are court records. The correction would be:

(2) All court records in civil cases, except those listed in (c)(1)–~~(9)~~(10).

(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 provide public remote ~~electronic~~ access only to the records ~~governed by~~ specified in subdivision (b):

(1)–(10) * * *

(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.

DRAFTER'S NOTE: The following comment was received in response to the proposed amendment of rule 2.503(e):

- Orange County Bar Association. 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.

Subcommittee and staff review: The comment is out of scope as it is unrelated to the proposed amendments. The proposed amendments to rule 2.503 make only technical changes to the existing rule.

(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

DRAFTER'S NOTE: The following comment was received in response to the proposed article 3 as a whole:

- Orange County Bar Association. 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.

Subcommittee and staff review: The comment is not specific enough to formulate an analysis or specific response. The commenter has not articulated why article 3 is "unnecessary, too redundant, too restrictive, and probably discriminatory."

Rule 2.515. Application and scope

(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.

(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 they would have if they were to seek to inspect the records in person at the courthouse. Thus, if they are legally entitled to inspect certain records at the courthouse, they could view the same records remotely; on the other hand, if they are restricted from inspecting certain court records at the courthouse (for example, because the records are confidential or sealed), they 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.

Drafter's Note: The following comments were received in response to the proposed adoption of rule 2.515:

- California Lawyers Association, The Executive Committee of the Trust and Estates Section. 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, 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
  (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.

Subcommittee and staff review: TEXCOM's suggestion would add clarity to the rules. The subcommittee recommends incorporating it into the proposal:

(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.

1 **Rule 2.516. Remote access to extent feasible**
2
3 To the extent feasible, a court that maintains records in electronic form must provide
4 remote access to those records to the users described in rule 2.515, subject to the
5 conditions and limitations stated in this article and otherwise provided by law.
6
7 **Advisory Committee Comment**
8
9 This rule takes into account the limited resources currently available in some trial courts. Many
10 courts may not have the financial means or the technical capabilities necessary to provide the full
11 range of remote access to electronic records authorized by this article. When it is more feasible
12 and courts have had more experience with remote access, these rules may be modified to further
13 expand remote access.
14
15 ***DRAFTER'S NOTE:*** The following comment was received in response to the
16 proposed adoption of rule 2.516:
17
18 - Joint Technology Subcommittee of the Trial Court Presiding Judges and
19 Court Executives Advisory Committees, and the Superior Court of
20 California, County of Placer. The language makes clear that courts may
21 provide varied remote access depending on their capabilities. However, as
22 written it is unclear whether it is ITAC's intent that courts refrain from
23 moving forward with any part of the remote access options until they can
24 move forward with all of the options. To avoid confusion and/or
25 unnecessary delays in implementation of some portions of remote access,
26 the rule could be modified to add:
27
28 Courts should provide remote access to the greatest extent feasible,
29 even in situations where all access outlined in these rules is not
30 feasible.
31
32 Alternatively, or in addition, we ask that ITAC consider adding a statement
33 to the Advisory Committee Comment to indicate: "This rule is not intended
34 to prevent a court from moving forward with limited remote access options
35 outlined in this rule as such access becomes feasible."
36
37 ***Subcommittee and staff review****:* Staff recommend the advisory committee
38 comment with the addition of an illustrative example. Article 3 is not meant to be
39 an all or none proposition as that is not a practical approach as it may not be
40 feasible for a court to add all the users outlined in rule 2.515 at once. The
41 subcommittee also discussed the "feasibility" standard in more detail and
42 suggested that "security resources" be added to the advisory committee

comment in addition to financial means and technical capabilities. The subcommittee recommended that the advisory committee comment read:

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 modified to further expand remote access.

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. 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 person), remote access would not apply to organizational parties, which would need to gain remote access through the party's attorney rule or, for certain government entities with respect to specified electronic records, the rules in article 4.

Drafter's Note: Staff recommend adding to the advisory committee comment to note that a person must have the legal capacity to agree to the terms and conditions of a user agreement. This is consistent with the subcommittee's recommendation with respect to rule 2.518, below. See subcommittee and staff review concerning age limits and capacity on pages 28-30, below. As modified, the advisory committee comment would be:

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 person), remote access would not apply to organizational parties, which would need to gain remote access through 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, e.g., 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 at least 18 years of age may designate other persons to have remote access to electronic records in actions or proceedings in which that person is a party.

(b) Level of remote access

(1) 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.

(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 person to authorize designees for remote access. Under rule 2.501, for purposes of the rules, "persons" are natural persons. Accordingly, the party designee rule would not apply to organizational parties, which would need to gain remote access through the party's attorney rule or, for certain government entities with respect to specified electronic records, the rules in article 4.

DRAFTER'S NOTE: The following comments were received in response to a request for specific comments on rule 2.518. The request for specific comments asked:

1) 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?

2) Should proposed rule 2.518 be limited to certain case types?

- Superior Court of California, County of Orange. *This comment was in response to the second question above.*

  Yes, the rule should be clear that it does not apply to juvenile justice and dependency case types.

- Superior Court of California, County of San Diego. *In response to the second question, the court said:* No.

  In response to the first question, the court commented: An emancipated or married minor should be exceptions for a person under 18 years of age. Additionally, should an exception be made for someone who is over 18 years of age but under a Conservatorship?

- Superior Court of California, San Joaquin. *This comment was in response to the first question above.*

  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.

  This comment was in response to the second question above.

  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 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.

Subcommittee and staff review: Regarding the 18 years of age cutoff, the subcommittee considered that the an age cut off is both underinclusive and over inclusive. It is underinclusive in denying remote access by persons under 18 who may have legal capacity to agree to it, and it is overinclusive in allowing remote access to persons over 18 who may not have legal capacity.

Ultimately, a party who is a person would have to have 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 (e.g., if identity verification revealed the person was a minor). Therefore, the subcommittee recommends removing the language "who is at least 18 years of age" from rule 2.518(a). As modified, the rule would be:

(a) Remote access generally permitted

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

The subcommittee also recommended adding in an advisory committee comment concerning capacity to agree to the terms and conditions of use of a remote access system. With that addition, the advisory committee comment would be:

Advisory Committee Comment

A party must be a natural person 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, "persons" are natural persons. Accordingly, the party designee rule would not apply to organizational parties, which would need to gain remote access through the party's attorney rule or, for certain government entities with respect to specified electronic records, the rules in article 4.

Staff recommend also that the advisory committee comment for rule 2.517 (remote access by a party) be revised similarly to include this information (see page 27, above)

Regarding limiting the types of records that can be access, the subcommittee recommends excluding remote access to court records related to juvenile and criminal matters. With respect to juvenile matters, the subcommittee was concerned about the sensitivity of the information, the fact that most of it is confidential, and noted that minors and parents should have counsel who will be able to gain remote access under other rules. With respect to criminal matters, the subcommittee was concerned about the sensitivity of the information and that a person could be subject to pressure from gangs to designate gang members to access the person's criminal records. To limit remote access to electronic records in juvenile (dependency and delinquency) and criminal matters, rule 2.518(b)(1) would be modified to state:

(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.

DRAFTER'S NOTE: The following comments were received in response to the proposed adoption of rule 2.518, but not in response to the request for specific comments.

- Joint Technology Subcommittee of the Trial Court Presiding Judges and Court Executives Advisory Committees, and the Superior Court of California, County of Placer. 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 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.

***Subcommittee and staff review**:* The subcommittee decided against making these modifications. Regarding making a clear statement that providing remote access under rule 2.518 is optional, this type of remote access is not optional if it is feasible to provide it. The commenters had previously raised a concern that article 3 could be read to require courts to only proceed with remote access if the court could provide it to all users under article 3. The amended comment to rule 2.516 on feasibility should clarify that. Accordingly, providing access to party designees under rule 2.518 is only required if feasible. If it is not feasible for a court to provide remote access to party designees—e.g. because insufficient financial resource, technical capacity, security resources—then the court does not need to provide access.

Regarding adding 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.

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 rule 2.518. If a party's attorney gains

remote access through 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 for attorneys who are not the attorney of record in the party's actions or proceedings in the trial court

An attorney who represents a party, but who is not the party's attorney of record, 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 the attorney has obtained the party's consent to remotely access the party's electronic records.

DRAFTER'S NOTE: The following comment was received in response to the proposed adoption of rule 2.519(c):

- Joint Technology Subcommittee of the Trial Court Presiding Judges and Court Executives Advisory Committees, and the Superior Court of California, County of Placer. 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 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 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.

Subcommittee and staff review*:* 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 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 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:

> 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.

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 subcommittee recommends adding an additional paragraph to the advisory committee comment to clarify this point. As amended, the advisory committee comment would be:

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. Examples include, but are not limited to, when a party engages 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/expungement 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 providing undisclosed representation from having to go to the courthouse.

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

1 adequate protections against data breaches then it would not be required, or if it
2 is not feasible for the court to provide differential access to attorneys of record vs.
3 other attorneys who have party consent then it would not be required. The
4 revision to the advisory committee comment on rule 2.516 concerning feasibility
5 makes clear that having adequate security resources can be part of whether
6 providing users access is feasible.
7
8 The commenters also state that "It is also unclear how the court would verify the
9 identity of the attorney who is not of record in this process." By design, the rules
10 do not prescribe any specific method for a court to use for identity verification. It
11 is something the court could do (e.g., require an attorney to appear at the court
12 and show their identification and bar card to get user credentials), require a legal
13 organization or qualified legal services project to do (e.g., require in an
14 agreement that the organization to do identity verification of its attorneys and
15 staff and provide that information to the court), or contract with an identity
16 verification service to do (e.g., a private company that is in the business of
17 identity verification). A court must verify identities to provide remote user access
18 under article 3, but if not feasible to do so, then the court does not need to
19 provide the remote access.
20
21 The comment about the release of liability relates to the party designee rule (rule
22 2.518) and is addressed in the analysis with that comment.
23
24 **(d) Terms of remote access for all attorneys accessing electronic records**
25
26 (1) A party's attorney may remotely access the electronic records only for the
27 purposes of assisting the party with the party's court matter.
28
29 (2) A party's attorney may not distribute for sale any electronic records obtained
30 remotely under the rules in this article. Such sale is strictly prohibited.
31
32 (3) A party's attorney must comply with any other terms of remote access
33 required by the court.
34
35 (4) Failure to comply with these rules may result in the imposition of sanctions,
36 including termination of access.
37
38 **Advisory Committee Comment**
39
40 **Subdivision (c).** An attorney of record will be known to the court for purposes of remote access.
41 However, a person may engage an attorney other than the attorney of record for assistance in an
42 action or proceeding in which the person is a party. Examples include, but are not limited to,
43 when a party engages an attorney to (1) prepare legal documents but not appear in the party's
44 action (e.g., provide limited-scope representation); (2) assist the party with

dismissal/expungement 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.

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.

Drafter's Note: The following comments were received in response to a request for specific comments on the term "legal organization" and "working in the same legal organization." The request for specific comments asked:

> 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?

- Superior Court of California, County of Orange. No, that is too broad a definition.

- Superior Court of California, County of San Diego. 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.

- Superior Court of California, County of San Joaquin. Yes it would and would add clarity to the rule.

Subcommittee and staff review: The subcommittee agrees with the comments that state "working at the direction of an attorney" is too broad and recommends retaining the wording "working in the same legal organization."

(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 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 subdivision (b) must be provided access to the same electronic records as the party.

(2) Notwithstanding subdivision (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.

DRAFTER'S NOTE: The following comments was received in response to the proposed adoption of rule 2.520:

- Joint Technology Subcommittee of the Trial Court Presiding Judges and Court Executives Advisory Committees, and the Superior Court of California, County of Placer. 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.

***Subcommittee and staff review**:* This seems reasonable. The rules do not prescribe any specific process, but the above could be an option. Certifying at one time and having that time be when the attorney establishes the remote access account is a logical time to name the other persons working in the same legal organization.

An advisory committee comment would read:

Advisory Committee Comment

The designation and certification outlined in (b) 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.

DRAFTER'S NOTE: The following comments were received in response to the proposed adoption of rule 2.521(a)(2):

- Superior Court of San Diego, County of San Diego. 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

Subcommittee and staff review: The subcommittee recommends against the additional citations as they do not speak to the court's power to appoint. Probate Code section 1894: does not confer separate, independent authority or duty on the court to appoint counsel. It imposes duties on the court investigator to determine whether the conservatee wishes to be represented, whether the conservatee has retained counsel, if not, whether the conservatee wants the court to appoint counsel, and then to report all those findings to the court. Probate Code section 2253 also imposes those duties on the investigator. It provides further that the conservatee has a right to be represented by counsel at the hearing, but it does not provide separate, independent authority for the court to appoint. Finally, Probate Code section 2356 bars the court from ordering certain placement or treatment of a conservatee, regardless of whether the conservatee has a lawyer. There are other Probate Code sections that do authorize or require appointment of counsel, but they all refer back to sections 1470, 1471, and 1474.

(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.

1 **Rule 2.522. Remote access by persons working in a qualified legal services project**
2 **providing brief legal services**
3
4 **(a) Application and scope**
5
6 (1) This rule applies to qualified legal services projects as defined in section
7 6213(a) of the Business and Professions Code.
8
9 (2) "Working in a qualified legal services project" under this rule includes
10 attorneys, employees, and volunteers.
11
12 (3) This rule does not apply to a person working in or otherwise associated with
13 a qualified legal services project who gains remote access to court records as
14 a party's designee under rule 2.518.
15
16 **(b) Designation and certification**
17
18 (1) A qualified legal services project may designate persons working in the
19 qualified legal services project who provide brief legal services, as defined in
20 article 1, to have remote access.
21
22 (2) The qualified legal services project must certify that the authorized persons
23 work in their organization.
24
25 **(c) Level of remote access**
26
27 Authorized persons may be provided remote access to the same electronic records
28 that the authorized person would be legally entitled to inspect at the courthouse.
29
30 **(d) Terms of remote access**
31
32 (1) Qualified legal services projects must obtain the party's consent to remotely
33 access the party's electronic records.
34
35 (2) Authorized persons must represent to the court in the remote access system
36 that the qualified legal services project has obtained the party's consent to
37 remotely access the party's electronic records.
38
39 (3) Qualified legal services projects providing services under this rule may
40 remotely access electronic records only to provide brief legal services.
41
42 (4) Any distribution for sale of electronic records obtained under the rules in this
43 article is strictly prohibited.

1
2 (5) All laws governing confidentiality and disclosure of court records apply to
3 electronic records obtained under this article.
4
5 (6) Qualified legal services projects must comply with any other terms of remote
6 access required by the court.
7
8 (7) Failure to comply with these rules may result in the imposition of sanctions,
9 including termination of access.
10
11 ***DRAFTER'S NOTE:*** The following comment was received in response to the
12 proposed adoption of rule 2.522:
13
14 - Joint Technology Subcommittee of the Trial Court Presiding Judges and
15 Court Executives Advisory Committees, and the Superior Court of
16 California, County of Placer. As written, this section appears to exempt
17 these agencies from the limitations of remote access to cases defined in
18 rule 2.503(c). The purpose of granting this exemption is unclear,
19 particularly in light of the other additions to the rule. For example, if rule
20 2.518 is adopted, this section may be unnecessary. Similarly, if rule, 2.519
21 is adopted, this section again may be unnecessary. Further, if rules 2.518
22 and 2.519 are not adopted, this rule presents additional concerns:
23
24 - 2.522(b) requires the legal services project to designate individuals
25 in their organization who have access, and certify that these
26 individuals work in their organization. It is unclear whether this
27 designation and certification is provided to the court or retained by
28 the organization. It is also unclear whether this designation or
29 certification is one-time, repeated, or must occur upon each access
30 to a case.
31 - 2.522(d)(1) states that the organization must have the party's
32 consent to remotely access the party's record. It is unclear how
33 such consent would be documented.
34 - 2.522(d)(2) creates a specific technical requirement that courts
35 would have to program into their remote access systems that
36 requires a self-representation of consent each time the authorized
37 person accesses a case. Unlike the other provisions of these rules,
38 that appear to contemplate a one-time designation, this section
39 would require an entirely new security layer at a "session" level to
40 ensure the authorized individual continues to certify their
41 authorization to access the case.
42

***Subcommittee and staff review**:* TCPJAC/CEAC states 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). 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.

TCPJAC/CEAC commented, "For example, if rule 2.518 is adopted, this section may be unnecessary." This is not the case however. 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 that may not be able to designate another under rule 2.518.

TCPJAC/CEAC commented, "Similarly, if rule, 2.519 is adopted, this section again may be unnecessary." 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.

TCPJAC/CEAC commented, "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." The designation would have to be provided to the court or the court would not know about it. This could be resolved through an advisory committee comment.

TCPJAC/CEAC commented, "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." The rule does not prescribe a particular record-keeping practice on the part of the qualified legal services project. If this needs to be addressed, it could be addressed in an advisory committee comment.

To address both of the above issues, the subcommittee recommends the following advisory committee comment:

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 both for both entities. Examples include: 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 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. Examples include: the qualified legal services project could obtain a signed consent form for its records, could obtain consent over the phone and make an entry to that effect in its records, or the court and qualified legal services project could enter an agreement to describe how consent will be obtained and recorded.

TCPJAC/CEAC commented, "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 require an entirely new 'security layer at a 'session" level to ensure the authorized individual continues to certify their authorization to access the case." This is likely how it would have to occur. When the rule was developed, the rule contemplated that brief legal services would often occur in high volume environments with a variety of clients seeking services. A court does not have to provide remote access to qualified legal services projects if it is not feasible to do so, e.g., because it is financially or technically not feasible at present.

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

(a) Identity verification required

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 proofing solution 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 by article 3 and 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, if a statewide identity verification, identity management, or access management system, or a statewide

1 master agreement for such systems is available, courts may use those for identity
2 verification, identity management, and user access services.
3
4 ***DRAFTER'S NOTE:*** The following comments was received in response to the
5 proposed adoption of rule 2.523:
6
7 - Joint Technology Subcommittee of the Trial Court Presiding Judges and
8 Court Executives Advisory Committees, and the Superior Court of
9 California, County of Placer. This section requires the court to verify the
10 identity of all users accessing court data. This requirement is
11 understandable when it relates to individuals who are known to the court
12 to be a part of the case being accessed. However, placing a requirement
13 on the court to verify the identity of individuals designated by the party to
14 access their case is overly burdensome and places the court in the
15 position to verify the identity of individuals unknown to the court.
16
17 We suggest adding language to clarify that the court is not required to
18 verify the identity of individuals granted access under rule 2.518, 2.519,
19 and 2.522 (if those sections remain). These rules grant access to cases by
20 individuals unknown to the court based solely upon the consent of the
21 party or by designation of third-parties. Under these conditions, the party
22 is consenting to access and the court should have no responsibility to
23 perform identify verification. Further, as previously stated, in all such
24 instances, the rules should clearly state that the party is removing the
25 court's responsibility for data security and confidentiality.
26
27 Subsections (a) and (d) appear to be in minor conflict. Suggest adding an
28 indication that (d) applies notwithstanding (a).
29
30 ***Subcommittee and staff review:*** In an early iteration, rule 2.518 did exempt
31 courts from the identity verification requirement as the thought at the time was
32 that the person designating would know who they were designating. Unlike
33 remote access by other third parties under article 3, the party designee rule
34 allows the party to directly communicate with the court about who should have
35 remote access to the party's electronic records. The other rules in article 3 do
36 not have a direct method for the party to communicate with the court. If it is
37 sufficient to assume that a party knows who he or she is designating, rule 2.523
38 could be amended to exempt courts from verifying the designee's identity.
39
40 A revised version of the rule could be:
41
42 **(a) Identity verification required**
43

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.

The subcommittee 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 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 done its due diligent to verify that a person is who they say they are).

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.

Subdivision (a) and (d) are not in conflict, but perhaps they are being read 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 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 subcommittee recommends clarifying this by adding the following advisory committee comment and staff recommend adding the same in the government entity context for rule 2.541 (that rule mirrors this rule):

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.

DRAFTER'S NOTE: The following comments was received in response to the proposed adoption of rule 2.524:

- Joint Technology Subcommittee of the Trial Court Presiding Judges and Court Executives Advisory Committees, and the Superior Court of California, County of Placer. We suggest adding an Advisory Committee Comment that specifies that data transmitted via HTTPS complies with the encryption requirement.

Subcommittee and staff review: 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, this may be better addressed through informational materials such as guidance documents or examples from courts.

1 **Rule 2.525. Searches and access to electronic records in search results**
2
3 **(a) Searches**
4
5 A user authorized under this article to remotely access a party's electronic records
6 may search for the records by case number or case caption.
7
8 **(b) Access to electronic records in search results**
9
10 A court providing remote access to electronic records under this article must ensure
11 that authorized users are able to access the electronic records only at the levels
12 provided in this article.
13
14 **(c) Unauthorized access**
15
16 If a user gains access to an electronic record that the user is not authorized to access
17 under this article, the user must:
18
19 (1) Report the unauthorized access to the court as directed by the court for that
20 purpose;
21
22 (2) Destroy all copies, in any form, of the record; and
23
24 (3) Delete from the user's browser history all information that identifies the
25 record.
26
27 **Rule 2.526. Audit trails**
28
29 **(a) Ability to generate audit trails required**
30
31 The court must have the ability to generate an audit trail that identifies each
32 remotely accessed record, when an electronic record was remotely accessed, who
33 remotely accessed the electronic record, and under whose authority the user gained
34 access to the electronic record.
35
36 **(b) Limited audit trails available to authorized users**
37
38 (1) A court providing remote access to electronic records under this article must
39 make limited audit trails available to authorized users under this article.
40
41 (2) A limited audit trail must show the user who remotely accessed electronic
42 records in a particular case but must not show which specific electronic
43 records were accessed.

Drafter's Note: The following comments were received in response to a request for specific comments on audit trails. The request for specific comments asked:

> 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?

- Superior Court of California, County of Orange. 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.

Subcommittee and staff review: The rule articulates what a limited audit trail is. It shows the user who remotely accessed the records in a particular case, but not show which specific electronic records were accessed. The audit trail is a tool to assist the courts in identifying and investigating any potential issues or misuse of remote access. The limited audit trail is a tool that can also assist parties and their attorneys in identifying potential issues with remote access. The view is limited, however, to protect sensitive information.

The subcommittee recommends adding an advisory committee comment that explains the purpose of the audit trails: This comment should also be included with rule 2.543, which governs audit trails under article 4 and is similar to rule 2.256. For example:

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.

- Superior Court of California, County of San Joaquin. Yes it would [present a challenge]. 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.

In response to the question, "is there a more feasible alternative?" the court commented: 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.

Subcommittee and staff review: It is not clear what "good cause" would be here. Requiring the users to request the report for "good cause" could reduce the number of reports that may need to be generated.

DRAFTER'S NOTE: The following comments were received in response to the proposed adoption of rule 2.526, but not in response to the request for specific comments.

- Joint Technology Subcommittee of the Trial Court Presiding Judges and Court Executives Advisory Committees, and the Superior Court of California, County of Placer. 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 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.

Subcommittee and staff review: TCPJAC/CEAC commented, "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." The requirement was added here is a mechanism to identify and address unauthorized data breaches. The controls that may be in place in the courthouse

for viewing a court record at a desk, or accessing an electronic record on the court's own computer, may not be present when external users are entering electronic systems. With the prevalence of data breaches in electronic systems in today's society, the ability to identify the source of a breach, trace the breach, and determine how widespread the breach is would be expected by the public and their elected representatives.

TCPJAC/CEAC suggests that the audit trail requirements, if kept, become permissive rather than mandatory so as not to halt existing services. One of the goals of the rules was to facilitate existing relationships and not create an obstacle to what courts are currently providing. The subcommittee recommends that the permissive language be adopted for audit trails and, accordingly, "must" be replaced with "should" for audit trails. (This would also alter rule 2.543, which is the audit trail requirement under article 4.) However, the audit trails may become mandatory in the future, especially as the remote access systems mature. The subcommittee recommends adding an advisory committee comment to his effect so that remote access systems are designed with that in mind. The advisory committee comment would be (in addition to the proposed language on the purpose of audit trails):

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.

While rule 2.526 is currently permissive to facilitate the use of existing remote access systems, the committee expects the rule will become mandatory in the future.

The commenters' recommendation that there be a defined retention period for audit records would be a sensible addition so courts do not have to retain the information indefinitely. This would need to be circulated for comment in an amendment to rule 2.256 in another rule cycle.

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 the imposition of 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

DRAFTER'S NOTE: The following comment was received in response to the proposed article 4 as a whole:

- Orange County Bar Association. The entirety of Article 4 has the same problems as Article 3 and suffers again from being unnecessary for these purposes.

Subcommittee and staff review: The Orange County Bar Association previously commented that article 3 was "unnecessary, too redundant, too restrictive, and probably discriminatory." Like that comment, the comment is not is not specific enough to formulate an analysis or specific response.

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 subdivision (b) below. 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 2–3.

(b) Level of remote access

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

1 (A) Office of the Attorney General: criminal electronic records and juvenile
2 justice electronic records.
3
4 (B) California Department of Child Support Services: family electronic
5 records, child welfare electronic records, and parentage electronic
6 records.
7
8 (C) Office of a district attorney: criminal electronic records and juvenile
9 justice electronic records.
10
11 (D) Office of a public defender: criminal electronic records and juvenile
12 justice electronic records.
13
14 (E) Office of a county counsel: criminal electronic records, mental health
15 electronic records, child welfare electronic records, and probate
16 electronic records.
17
18 (F) Office of a city attorney: criminal electronic records, juvenile justice
19 electronic records, and child welfare electronic records.
20
21 (G) County department of probation: criminal electronic records, juvenile
22 justice electronic records, and child welfare electronic records.
23
24 (H) County sheriff's department: criminal electronic records and juvenile
25 justice electronic records.
26
27 (I) Local police department: criminal electronic records and juvenile
28 justice electronic records.
29
30 (J) Local child support agency: family electronic records, child welfare
31 electronic records, and parentage electronic records.
32
33 (K) County child welfare agency: child welfare electronic records.
34
35 (L) County public guardian: criminal electronic records, mental health
36 electronic records, and probate electronic records.
37
38 (M) County agency designated by the board of supervisors to provide
39 conservatorship investigation under chapter 3 of the Lanterman-Petris-
40 Short Act (Welf. & Inst. Code, §§ 5350–5372): criminal electronic
41 records, mental health electronic records, and probate electronic
42 records.
43

(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 2–3.

DRAFTER'S NOTE: The following comments were received in response to a request for specific comments on the term "concurrent jurisdiction" used in rule 2.540(b)(1)(N). The request for specific comments asked:

> 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?

- Superior Court of California, County of Orange. Concurrent jurisdiction should be defined within the rule itself.

- Superior Court of California, County of San Diego. The phrase "concurrent jurisdiction" is sufficient to describe these scenarios.

- Superior Court of California, County of San Joaquin. 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".

Subcommittee and staff review: The subcommittee recommends the rule as circulated. The Superior Court of California, County of San Diego's comment that it is sufficient is particularly persuasive as a large number of tribes are located in San Diego County. The tribes and courts may be able to resolve the meaning through agreements.

DRAFTER'S NOTE: The following comments were received in response to a request for specific comments on the term "good cause" used in rule 2.540(b)(1)(O). The request for specific comments asked, "Is the standard for "good cause" in proposed rule 2.540(b)(1)(O) clear?"

- Superior Court of California, County of Orange. Yes.

- Superior Court of California, County of San Diego. Yes.

- Superior Court of California, County of San Joaquin Yes, it is.

DRAFTER'S NOTE: The following comments were received in response to the proposed adoption of rule 2.540(b)(1), but not in response to the request for specific comments.

- Superior Court of San Diego, County of San Diego. 2.521(a)(2): Proposes that Public Administrator and Public Conservator be added to the list of authorized persons from government entities that may be provided remote access to electronic records.

Subcommittee and staff review: The subcommittee anticipated that additions to the list may be required. While the public guardian, public administrator, and public conservator are often the same person, some counties may split the duties of these roles. The subcommittee recommends that this be made a part of a proposal to amend the remote access rules in a future rules cycle, but in the interim, the "good cause" provision should allow courts to grant remote access to public administrators and public conservators.

- California Child Support Director's Association. 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 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 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 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.

Subcommittee and staff review: The subcommittee recommends the language in rule 2.540(b) remain permissive on the part of the court.

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. The proposed rule would need to be recirculated for public comment if changed to be mandatory.

- California Department of Child Support Services. 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.

1
2 The Department recognizes that the JCC cannot impose a requirement
3 that all courts provide remote access to their high-volume justice partners
4 at this time due to the lack of a single statewide court case management
5 system. However, there is an opportunity for the JCC to promote greater
6 court access for high volume justice partners than is contemplated by the
7 permissive rule as drafted. More specifically, the Department would
8 encourage the JCC to consider amending the rule to mandate that trial
9 courts provide remote access to local court case management systems
10 when feasible.
11
12 The Department also appreciates formal recognition by the JCC that
13 remote access to multiple case types supports the ability of the child
14 support program, as a whole, to discharge its state and local mandates
15 effectively. Such access helps the Department provide vitial [sic]
16 information about all court orders entered in California to the Federal
17 Parent Locator System. Remote access is also valuable because it
18 permits local child support agencies to have timely access to information
19 about any onoing in-state court proceedings and the existence of
20 California parentage and child support judgments. Access to this vital case
21 information helps ensure that local child support agencies do not ask
22 courts to enter conflicting or void child support judgments.·
23
24 That said, the Department has concerns that the rule, as drafted, may not
25 achieve statewide uniformity for the child support program as the JCC
26 appears to intend. To amerilorate this risk, the Department respectfully
27 requests that the JCC consider amending the child support provisions of
28 Rule 2.540(b)(1) in two ways.
29
30 First, under California law, both the Department and all child support
31 agencies have the same right to access this type of information. By
32 creating two separate subparts, the rule seems to suggest these two
33 governmental entities may be treated differently. This problem could be
34 avoided by combining (b)(1)(B) an (b)(1)(J) into a single exception, as
35 follows:
36
37 (b)(1)(B) California Department of Child Support Services *and local*
38 *child support agencies*: family electronic records, child welfare
39 electronic records, and parentage electronic records.
40
41 Second, while it appears the JCC intends to ensure that the Department
42 and LCSAs have electronic access to filings under Family Code Section
43 17404, and the Uniform Parentage Act (UPA), as provided by Family
44 Code section 7643, the term "parentage" may be narrowly construed by
45 some courts. As such, the Department respectfully requests that the term
46 "parentage electronic records" be defined 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. *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 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 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 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.

Subcommittee and staff review: The subcommittee recommends that (1) the language in rule 2.540(b) remain permissive on the part of the court, (2) access by California Department of Child Support Services and local child support agencies remain in separate rules, (3) an advisory committee comment be added to clarify that courts may allow access for local government entities in different counties than where the court is situated, and (4) a non-exhaustive list of authorities for "parentage" not be included with rules where "parentage electronic records" may be accessed remotely, and (5) the rules not be modified to address fees.

With respect to making rule 2.540 mandatory rather than permissive, the rule was designed to be 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.

With respect to incorporating access by California Department of Child Support Services and local child support agencies in the same rule, staff recommend against this because the rules were intentionally organized by each individual government entity. This is not just for organizational ease, but also so courts accommodate each entity with remote access as the court's business needs and capacity dictate. 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.

With respect to adding an advisory committee comment, the California Department of Child Support Services had suggested that "local child support agency" in rule 2.540(b)(1(J) be changed to "local child support agencies" so that a local child support agency in one county could potentially remotely access electronic records of the court situated in another county (rather than the court only dealing with the local child support agency in the county where the court was located). The subcommittee recommends adding an advisory committee comment on this subject rather than modifying the proposed rule. This could apply to other local-level government entities as well. While 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 resides, the following advisory committee comment could provide greater clarity on this topic:

Advisory Committee Comment

The rule does not restrict courts to only providing remote access 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.

With respect to adding authorities governing "parentage" where access may be allowed "parentage electronic records," the subcommittee recommends against the language suggested by California Department of Child Support Services as it is unnecessary.

Finally, the subcommittee recommend against adding the proposed language concerning fees. Access 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.

(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

Subdivision (b)(3). On 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 proofing solution 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 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.

1 **(d) Responsibilities of government entities**
2
3 (1) If a person is accessing electronic records on behalf of a government entity,
4 the government entity must approve granting access to that person, verify the
5 person's identity, and provide the court with all the information it needs to
6 authorize that person to have access to electronic records.
7
8 (2) If a person accessing electronic records on behalf of a government entity
9 leaves his or her position or for any other reason is no longer entitled to
10 access, the government entity must immediately notify the court so that it can
11 terminate the person's access.
12
13 **(e) Vendor contracts, statewide master agreements, and identity and access**
14 **management systems**
15
16 A court may enter into a contract with a vendor to provide identity verification,
17 identity management, or user access services. Alternatively, if a statewide identity
18 verification, identity management, or access management system or a statewide
19 master agreement for such systems is available, courts may use those for identity
20 verification, identity management, and user access services.
21
22 **Rule 2.542. Security of confidential information**
23
24 **(a) Secure access and encryption required**
25
26 If any information in an electronic record that is confidential by law or sealed by
27 court order may lawfully be provided remotely to a government entity, any remote
28 access to the confidential information must be provided through a secure platform,
29 and any electronic transmission of the information must be encrypted.
30
31 **(b) Vendor contracts and statewide master agreements**
32
33 A court may enter into a contract with a vendor to provide secure access and
34 encryption services. Alternatively, if a statewide master agreement is available for
35 secure access and encryption services, courts may use that master agreement.
36
37 **Rule 2.543. Audit trails**
38
39 **(a) Ability to generate audit trails required**
40
41 The court must have the ability to generate an audit trail that identifies each
42 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.

(b) Audit trails available to government entity

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

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

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 protect itself from 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 under this article is a privilege and not a right.

(b) Termination by court

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

Comments Responsive to the Request for Specific Comments:
The following comments were received in response to the request for specific comments and were not tied to any particular rule.

Question: Does the proposal appropriately address the stated purpose?

Answers:

- Superior Court of California, County of San Diego. Yes.

Question: 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, 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?

Answers:

- Superior Court of California, County of San Diego. The included language is clear and reduces the need for the user to refer to additional rules.

- Superior Court of California, County of San Joaquin Yes, it does.

Question: 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?

Answers:

- Superior Court of California, County of Orange. This is dependent upon whether or not courts have existing applications that allow remote access.

- Superior Court of California, County of San Diego. ? In order to be able to answer this question, our 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 California, County of San Joaquin. 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:
  - 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.

Subcommittee and staff review: The comments on implementation requirements will be included with the Judicial Council report.

Question: What implementation guidance, if any, would courts find helpful?

Answers:

- Superior Court of California, County of Orange. A quick reference.

- Superior Court of California, County of San Diego. A governance and best practice checklist for implementing remote access.

- Superior Court of California, County of San Joaquin. 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 if it is feasible for the court to follow through with implementation of remote records access.

Question: Would the proposal provide cost savings? If so, please quantify.

Answers:

- Superior Court of California, County of Orange. 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 California, County of Orange. No.

- Superior Court of California, County of San Joaquin. 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.

Subcommittee and staff review: The comments on costs will be included with the Judicial Council report.

Other Comments:

The following comments were not in response to any specified rule or request for specific comments, but applied more broadly to the proposal.

- Joint Technology Subcommittee of the Trial Court Presiding Judges and Court Executives Advisory Committees, and the Superior Court of California, County of Placer. 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 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.

Subcommittee and staff review: The comments on impacts on case management systems, workload, and security will be included with the Judicial Council report.

- The Orange County Bar Association. 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 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.

***Subcommittee and staff review*:** It is not clear from the comments what is "possibly unconstitutional" and "contradictory" about the proposed rules. The "limited amendments" referenced in the executive summary of the invitation to comment were with respect to the public access rules. As the executive summary also noted, the proposal creates a new set of rules as well. The amendments to the public access rules do not substantively alter the methods of access by the public (in the courthouse or remotely). 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.

- Superior Court of California, County of Orange. 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?

Subcommittee and staff review: 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 represent that to the court; the court would not need to take additional steps to independently verify the identities.)

- Superior Court of California, County of San Bernardino. 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).

  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.

***Subcommittee and staff review*:** 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.

Regarding the level of remote access, the court did not specify which rule it was referring to, but it is likely 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.

- Timothy Cassidy-Curtis. 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, 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 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.

Subcommittee and staff review: The proposed rules do not require the courts to certify electronic records to which they provide remote access though courts could do so in light of statutory authority to certify electronic records under Government Code section 69150(f):

> A copy of a court record created, maintained, preserved, or reproduced according to subdivisions (a) and (c) shall be deemed an original court record and may be certified as a true and correct copy of the original record. The clerk of the court may certify a copy of the record by electronic or other technological means, if the means adopted by the court reasonably ensures that the certified copy is a true and correct copy of the original record, or of a specified part of the original record.

- Tulare County Public Guardian's Office. The proposed changes clarify and expand on the existing rules. I personal approve of these changes.

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] 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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] 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	

2

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] 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): <u>(1) A court shall provide authorized persons from government entities with remote access to electronic records as follows:</u> 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	

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] 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	

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] 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. <u>Rule 2.540</u>	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.

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] 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

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] 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.

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] 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	

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] 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:	

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] 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	

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] 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	

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] 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	

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] 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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] Committee Response
	<u>TEXCOM</u> Ellen McKissock Hopkins & Carley Tel: 408-286-9800 E-mail: emckissock@hopkinscarley.com <u>California Lawyers Association</u> 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**	

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] 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).

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] 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	

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] 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.

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] 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 out of scope 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.

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] 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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] 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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] 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.*	The comments on costs will be included with the Judicial Council report. The committee will add an advisory committee comment explaining the purpose of the audit trail.

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] 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.*	

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] 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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] 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. Regarding the level of remote access, the committee assumes the comment is in reference to rule

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] 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).	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.

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] 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.	
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 under 18 years of age. Additionally, should an exception be made for	The committee appreciates the responses to the request for specific comments. They are helpful and insightful information for committee to consider. 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. The comments on 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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] Committee Response
			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 would only be during the case initiation phase, when in reality they could obtain assistance throughout the life of a case.	Regarding rule 2.521, the committee declines to add the additional citations they do not confer separate, independent authority or duty on the court to appoint. Regarding rule 2.540(b), 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.

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] Committee Response
			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 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	

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] Committee Response
			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, 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	

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] Committee Response
			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: 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	

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] Committee Response
			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? 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	

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] Committee Response
			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. General Comments: **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 provided remote access to electronic records.	
11	Superior Court of California, County of San Joaquin Erica A Ochoa	NI	Does the proposal appropriately address the stated purpose?	The committee appreciates the responses to the specific comments as they are helpful in determining

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] Committee Response
	Records Manager 540 E Main Street Stockton CA 95202 Tel: 209-992-5221 eochoa@sjcourts.org		• 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 unlimited access it is very difficult to convince the public you are not hiding something by taking choices away. The question of transparency	the committee's recommendation to the council. Regarding over 18 access, 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. Comments on the costs and implementation will be included with the Judicial Council report. Regarding the audit trail, the committee declines to add "good cause" language. The committee has instead made the audit trail permissive rather than mandatory.

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] Committee Response
			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. 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"	

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] Committee Response
			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. • 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	

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] Committee Response
			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 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	

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] Committee Response
			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 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	

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] Committee Response
			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. 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	

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] Committee Response
			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 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	

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] Committee Response
			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.	
12	TCPJAC/CEAC Joint Rules Subcommittee (JRS) By Corey Rada, Senior Analyst Judicial Council and Trial Court Leadership | Leadership Services Division	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	The committee appreciates the comments. The comments on impacts on case management systems, workload, and security will be included with the Judicial Council report.

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] Committee Response
	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		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 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	Regarding rule 2.501, the suggested modification is clearer and the committee will recommend it. 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 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

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] Committee Response
			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** ○ Modify the definition of "court case information" to use more natural language to reduce confusion. A possible definition might be: "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	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 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

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] Committee Response
			the action and is not part of the official court record for the case or cases. • **Rule 2.503(b)(2)** ○ "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** ○ 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 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*	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 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

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] Committee Response
			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 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,	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 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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] Committee Response
			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** ○ 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 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	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. 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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] Committee Response
			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 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	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. 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.

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] Committee Response
			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 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	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). 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.

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] Committee Response
			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.** ○ 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: ▪ 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	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 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.

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] Committee Response
			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 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**	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/disagrees, TBD at the July 2 ITAC meeting] with exempting courts from verifying the identities of users 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

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] Committee Response
			verification, identity management, and user access ○ 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 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	(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 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 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

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] Committee Response
			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** 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	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 perhaps they are ambiguous or being read 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 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

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[**DRAFT**] Committee Response
			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 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	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 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

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

ITC SPR18-37
Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	[DRAFT] Committee Response
			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.	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.

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