



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	Action Requested
July 5, 2018	Please review
To	Deadline
Judicial Council Technology Committee, Hon. Marsha G. Slough, Chair	July 9, 2018
From	Contact
Andrea L. Jaramillo Attorney, Legal Services	Andrea L. Jaramillo 916-263-0991 phone andrea.jaramillo@jud.ca.gov
Subject	
Rules and Forms Recommended by the Information Technology Advisory Committee	

Background

On July 2, 2018, the Information Technology Advisory Committee (ITAC) met to consider public comments and vote on recommending rules and forms proposals for Judicial Council amendment and adoption. Prior to the ITAC meeting and in anticipation of the Judicial Council Technology Committee (JCTC) meeting on July 9, 2018, JCTC received copies of the same materials that ITAC received. This memorandum includes an update on the results of the ITAC meeting and an attachment of supplemental materials.

ITAC Meeting Results

A. ITAC Recommended the Electronic Filing and Service Rules Proposal for Consideration by JCTC and Adoption by the Judicial Council

ITAC recommended the rules proposal that would amend rules related to electronic service and electronic filing, specifically rules 2.250, 2.251, 2.252, 2.253, 2.254, 2.255, 2.256, 2.257, and 2.259. New provisions of Code of Civil Procedure section 1010.6 (section 1010.6) requiring express consent for electronic service necessitate conforming changes to the rules of court. Additional 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 proposal received feedback from four commenters, three of which responded with substantive comments. ITAC considered the comments and proposal on July 2, 2018 and recommended the proposal for Judicial Council adoption.

B. ITAC and the Civil and Small Claims Advisory Committee Recommended the Form Proposal, *Withdrawal of Consent to Electronic Service*, for Consideration by JCTC and Adoption by the Judicial Council

ITAC and the Civil and Small Claims Advisory Committee (CSCAC) circulated a joint proposal for new form EFS-006, *Withdrawal of Consent to Electronic Service*. The purpose of form 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.

Four commenters submitted comments, which the CSCAC considered at its June 27, 2018 meeting and ITAC at its July 2, 2018 meeting. Both committees agreed with a suggestion from the Superior Court of California, County of Los Angeles that the form should include a notice that the form does not apply when electronic service is mandatory. Accordingly, the committees recommended the proposal for Judicial Council adoption with the inclusion of a notice that the form may not be used for mandatory electronic service required by local rule or court order.

C. ITAC Recommended the Remote Access to Electronic Records Rules Proposal for Consideration by JCTC and Adoption by the Judicial Council

ITAC recommended the proposal, which makes limited amendments to existing 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, 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.

Thirteen commenters submitted comments in response to the invitation to comment. The Joint Ad Hoc Subcommittee on Remote Access recommended modifications based on comments received and discussion of the subcommittee. ITAC discussed the comments and subcommittee recommendations at its July 2, 2018 meeting and made additional modifications and recommend the proposal for JCTC consideration and Judicial Council adoption. The most significant points of discussion that resulted in modifications at ITAC's meeting were rule 2.523 (identity verification) and rule 2.526 (audit trail).

For rule 2.523, the Joint Technology Subcommittee of the Trial Court Presiding Judges Advisory Committee (TCPJAC) and Court Executives Advisory Committee (CEAC) and Superior Court of California, County of Placer recommended that courts not be required to verify the identities of party designees granted remote access under rule 2.518. ITAC agreed with this recommendation. Unlike remote access by other third parties under article 3, the party designee rule allows the party to directly communicate with the court about who should have remote access to the party's electronic records. The parties themselves are able to control who gains access under the party designee rule, which mitigates concerns about unknown third persons gaining unauthorized remote access.

For rule 2.526, the Joint Technology Subcommittee of TCPJAC/CEAC and the Superior Court of California, County of Placer recommended that the audit trail requirement be non-mandatory rather than mandatory. ITAC had solicited comments on whether the audit trail requirement would present a challenge and whether there were more feasible alternatives. TCPJAC/CEAC commented, "The current mandatory language may result in a court being prohibited from providing any electronic access even with the ability to do so, if the court does not have the ability to provide the required audit trail." A goal of the rules proposal is to facilitate current use of remote access rather than inhibit it. Accordingly, ITAC agreed and recommended making rule 2.526 non-mandatory and adding an advisory committee comment that the committee expects the rule will become mandatory in the future. ITAC can circulate an amendment in another rule cycle to provide for and seek feedback on potential dates for a deadline to be incorporated into the rule. Article 4 has a mirror audit trail requirement under rule 2.543, which

applies to remote access by government entities and ITAC recommended making equivalent changes to that rule.

ITAC recommended the proposal with additional modifications recommended by the Joint Ad Hoc Subcommittee on Remote Access and staff. The complete list of modifications is below.

1. **Rule 2.502(4).** Revise the wording of the “court case information” definition to use clearer plain language.
2. **Rule 2.503(b)(2).** Make a technical correction consistent with the rest of the rules by adding “court” to “all records” so it states “all court records.”
3. **Rule 2.515(a).** Add a clarifying sentence at the end of subdivision (a) that states, “These rules govern access to electronic records where remote access by the public is not allowed.” This information is also conveyed in detail in the advisory committee comment, but the rule itself is clearer with the addition to subdivision (a).
4. **Rule 2.516.**
 - a. Add “security resources” to the advisory committee comment as an element to consider when assessing feasibility of providing remote access.
 - b. Add an explanation to the advisory committee comment that the rule is not intended to prevent a court from moving forward with limited remote access options if it is not feasible to provide remote access to all users identified in article 3.
5. **Rule 2.517.** Add to the advisory committee comment that a person must have legal capacity to agree to the terms and conditions of a user agreement of a remote access system.
6. **Rule 2.518.**
 - a. Strike “who is at least 18 years of age” from subdivision (a) because the age cut off is both underinclusive (e.g., excluding emancipated minors) and overinclusive (e.g., including adults under conservatorship). The legal capacity to agree to terms and conditions of a user agreement allowing use of a remote access system is the crux of who may designate. Add an advisory committee comment instead that a person designating must have legal capacity to agree to the terms and conditions of a user agreement.
 - b. Carve out an exception to remote access by designee in subdivision (b)(1) to disallow access to criminal electronic records because of the sensitivity of the information combined with the potential for a person to be subject to pressure from gangs to designate gang members to be allowed remote access to the person’s criminal records.
 - c. Carve out an exception to remote access by a designee in subdivision (b)(1) to disallow access to juvenile justice and child welfare records because of the

sensitivity of the information combined with the fact that counsel are typically involved and minors' and parents' attorneys can gain access under other rules.

7. **Rule 2.519(c).** Add to the an advisory committee comment to provide more clarification about the level of access an undisclosed attorney providing limited scope representation (as opposed to an attorney providing noticed limited scope representation) can gain through remote access.
8. **Rule 2.520(b).** Add an advisory committee comment that designation and certification can be done once and at the time the attorney establishes his or her remote access account with the court.
9. **Rule 2.522.** Add an advisory committee comment clarifying that the courts and qualified legal services projects have flexibility in determining an appropriate process for capturing designation and certification and for recordkeeping.
10. **Rule 2.523.**
 - a. Add an exception to subdivision (a) for remote access provided to a party's designee under rule 2.518.
 - b. Add an advisory committee comment clarifying that a court can use subdivision (d) to meet the identity verification requirements of subdivision (a).
11. **Rule 2.526.**
 - a. Modify the rule so that it is not mandatory.
 - b. Add an advisory committee comment explaining the purpose of the audit trail and setting an expectation that the rule will become mandatory in the future.
12. **Rule 2.540.** Add an advisory committee comment to clarify that the rules does not restrict courts to providing remote access only to local government entities in the same county in which the court is situated.
13. **Rule 2.543.**
 - a. Modify the rule so that it is not mandatory.
 - b. Add an advisory committee comment explaining the purpose of the audit trail and setting an expectation that the rule will become mandatory in the future.

A copy of the rules with all recommendations incorporated is attached to this memorandum along with a revised chart of comments.

Recommendations

Recommend the rule and form proposals for Judicial Council adoption at its September 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 7-31
2. Chart of comments, at pages 32-84.

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:

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

2
3 **Article 1. General Provisions**

4
5 **Rule 2.500. Statement of purpose**

6
7 **(a) Intent**

8
9 The rules in this chapter are intended to provide the public, parties, parties’
10 attorneys, legal organizations, court-appointed persons, and government entities
11 with reasonable access to trial court records that are maintained in electronic form,
12 while protecting privacy interests.

13
14 **(b) Benefits of electronic access**

15
16 Improved technologies provide courts with many alternatives to the historical
17 paper-based record receipt and retention process, including the creation and use of
18 court records maintained in electronic form. Providing ~~public~~ access to trial court
19 records that are maintained in electronic form may save the courts, ~~and the public,~~
20 parties, parties’ attorneys, legal organizations, court-appointed persons, and
21 government entities time, money, and effort and encourage courts to be more
22 efficient in their operations. Improved access to trial court records may also foster
23 in the public a more comprehensive understanding of the trial court system.

24
25 **(c) No creation of rights**

26
27 The rules in this chapter are not intended to give the public, parties, parties’
28 attorneys, legal organizations, court-appointed persons, and government entities a
29 right of access to any record that they are not otherwise legally entitled to access.
30 ~~The rules do not create any right of access to records that are sealed by court order~~
31 ~~or confidential as a matter of law.~~

32
33 **Advisory Committee Comment**

34
35 The rules in this chapter acknowledge the benefits that electronic ~~court~~ records provide but
36 attempt to limit the potential for unjustified intrusions into the privacy of individuals involved in
37 litigation that can occur as a result of remote access to electronic ~~court~~ records. The proposed
38 rules take into account the limited resources currently available in the trial courts. It is
39 contemplated that the rules may be modified to provide greater electronic access as ~~the~~ courts’
40 technical capabilities improve and ~~with the~~ knowledge is gained from the experience of ~~the courts~~
41 ~~in~~ providing electronic access under these rules.

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 **Advisory Committee Comment**

25
26 The rules on remote access do not apply beyond court records to other types of documents,
27 information, or data. Rule 2.502 defines a court record as “any document, paper, or exhibit filed
28 in an action or proceeding; any order or judgment of the court; and any item listed in Government
29 Code section 68151(a), excluding any reporter’s transcript for which the reporter is entitled to
30 receive a fee for any copy. The term does not include the personal notes or preliminary
31 memoranda of judges or other judicial branch personnel, statutorily mandated reporting between
32 government entities, judicial administrative records, court case information, or compilations of
33 data drawn from court records where the compilations are not themselves contained in a court
34 record.” (Rule 2.502(4), Cal. Rules of Court.) Thus, courts generate and maintain many types of
35 information that are not court records and to which access may be restricted by law. Such
36 information is not remotely accessible as court records, even to parties and their attorneys. If
37 parties and their attorneys are entitled to access to any such additional information, separate and
38 independent grounds for that access must exist.

39
40 **Rule 2.502. Definitions**

41
42 As used in this chapter, the following definitions apply:

- 1 (1) “Authorized person” means a person authorized by a legal organization, qualified
 2 legal services project, or government entity to access electronic records.
 3
- 4 (2) “Brief legal services” means legal assistance provided without, or before, becoming
 5 a party’s attorney. It includes giving advice, having a consultation, performing
 6 research, investigating case facts, drafting documents, and making limited third-
 7 party contacts on behalf of a client.
 8
- 9 ~~(1)~~(3) “Court record” is any document, paper, or exhibit filed by the parties to in an action
 10 or proceeding; any order or judgment of the court; and any item listed in
 11 Government Code section 68151(a),—excluding any reporter’s transcript for which
 12 the reporter is entitled to receive a fee for any copy—that is maintained by the court
 13 in the ordinary course of the judicial process. The term does not include the
 14 personal notes or preliminary memoranda of judges or other judicial branch
 15 personnel, statutorily mandated reporting between or within government entities,
 16 judicial administrative records, court case information, or compilations of data
 17 drawn from court records where the compilations are not themselves contained in a
 18 court record.
 19
- 20 (4) “Court case information” refers to data that is stored in a court’s case management
 21 system or case histories. This data supports the court’s management or tracking of
 22 the action and is not part of the official court record for the case or cases.
 23
- 24 ~~(4)~~(5) “Electronic access” means ~~computer~~ access by electronic means to court records
 25 available to the public through both public terminals at the courthouse and
 26 remotely, unless otherwise specified in the rules in this chapter.
 27
- 28 ~~(2)~~(6) “Electronic record” is a ~~computerized~~ court record, regardless of the manner in
 29 which it has been computerized that requires the use of an electronic device to
 30 access. The term includes both a ~~document~~ record that has been filed electronically
 31 and an electronic copy or version of a record that was filed in paper form. The term
 32 does not include a court record that is maintained only on microfiche, paper, or any
 33 other medium that can be read without the use of an electronic device.
 34
- 35 (7) “Government entity” means a legal entity organized to carry on some function of
 36 the State of California or a political subdivision of the State of California. A
 37 government entity is also a federally recognized Indian tribe or a reservation,
 38 department, subdivision, or court of a federally recognized Indian tribe.
 39
- 40 (8) “Legal organization” means a licensed attorney or group of attorneys, nonprofit
 41 legal aid organization, government legal office, in-house legal office of a
 42 nongovernmental organization, or legal program organized to provide for indigent
 43 criminal, civil, or juvenile law representation.

1
2 (9) “Party” means a plaintiff, defendant, cross-complainant, cross-defendant,
3 petitioner, respondent, intervenor, objector, or anyone expressly defined by statute
4 as a party in a court case.

5
6 (10) “Person” means a natural human being.

7
8 ~~(3)~~(11) “The public” means an individual a person, a group, or an entity, including print
9 or electronic media, or the representative of an individual, a group, or an
10 entity regardless of any legal or other interest in a particular court record.

11
12 (12) “Qualified legal services project” has the same meaning under the rules of this
13 chapter as in 6213(a) of the Business and Professions Code.

14
15 (13) “Remote access” means electronic access from a location other than a public
16 terminal at the courthouse.

17
18 (14) “User” means an individual person, a group, or an entity that accesses electronic
19 records.

20 21 Article 2. Public Access

22 23 **Rule 2.503. Public access Application and scope**

24 25 **(a) General right of access by the public**

26
27 (1) All electronic records must be made reasonably available to the public in
28 some form, whether in electronic or in paper form, except those that are
29 sealed by court order or made confidential by law.

30
31 (2) The rules in this article apply only to access to electronic records by the
32 public.

33 34 **(b) Electronic access required to extent feasible**

35
36 A court that maintains the following records in electronic form must provide
37 electronic access to them, both remotely and at the courthouse, to the extent it is
38 feasible to do so:

39
40 (1) * * *

41
42 (2) All court records in civil cases, except those listed in (c)(1)–~~(9)~~(10).

43

1 (c) **Courthouse electronic access only**

2
3 A court that maintains the following records in electronic form must provide
4 electronic access to them at the courthouse, to the extent it is feasible to do so, but
5 may provide public remote ~~electronic~~ access only to the records governed by
6 specified in subdivision (b):

7
8 (1)–(10) * * *

9
10 (d) * * *

11
12 (e) **Remote ~~electronic~~ access allowed in extraordinary criminal cases**

13
14 Notwithstanding (c)(5), the presiding judge of the court, or a judge assigned by the
15 presiding judge, may exercise discretion, subject to (e)(1), to permit remote
16 ~~electronic~~ access by the public to all or a portion of the public court records in an
17 individual criminal case if (1) the number of requests for access to documents in
18 the case is extraordinarily high and (2) responding to those requests would
19 significantly burden the operations of the court. An individualized determination
20 must be made in each case in which such remote ~~electronic~~ access is provided.

21
22 (1) In exercising discretion under (e), the judge should consider the relevant
23 factors, such as:

24
25 (A) * * *

26
27 (B) The benefits to and burdens on the parties in allowing remote ~~electronic~~
28 access, including possible impacts on jury selection; and

29
30 (C) * * *

31
32 (2) The court should, to the extent feasible, redact the following information
33 from records to which it allows remote access under (e): driver license
34 numbers; dates of birth; social security numbers; Criminal Identification and
35 Information and National Crime Information numbers; addresses and phone
36 numbers of parties, victims, witnesses, and court personnel; medical or
37 psychiatric information; financial information; account numbers; and other
38 personal identifying information. The court may order any party who files a
39 document containing such information to provide the court with both an
40 original unredacted version of the document for filing in the court file and a
41 redacted version of the document for remote ~~electronic~~ access. No juror
42 names or other juror identifying information may be provided by remote
43 ~~electronic~~ access. This subdivision does not apply to any document in the

1 original court file; it applies only to documents that are available by remote
2 ~~electronic~~ access.

3
4 (3) Five days' notice must be provided to the parties and the public before the
5 court makes a determination to provide remote ~~electronic~~ access under this
6 rule. Notice to the public may be accomplished by posting notice on the
7 court's ~~Web site~~ website. Any person may file comments with the court for
8 consideration, but no hearing is required.

9
10 (4) The court's order permitting remote ~~electronic~~ access must specify which
11 court records will be available by remote ~~electronic~~ access and what
12 categories of information are to be redacted. The court is not required to
13 make findings of fact. The court's order must be posted on the court's ~~Web~~
14 site website and a copy sent to the Judicial Council.

15
16 **(f)–(i)** * * *

17
18 **Advisory Committee Comment**

19
20 The rule allows a level of access by the public to all electronic records that is at least equivalent
21 to the access that is available for paper records and, for some types of records, is much greater. At
22 the same time, it seeks to protect legitimate privacy concerns.

23
24 **Subdivision (c).** This subdivision excludes certain records (those other than the register, calendar,
25 and indexes) in specified types of cases (notably criminal, juvenile, and family court matters)
26 from public remote ~~electronic~~ access. The committee recognized that while these case records are
27 public records and should remain available at the courthouse, either in paper or electronic form,
28 they often contain sensitive personal information. The court should not publish that information
29 over the Internet. However, the committee also recognized that the use of the Internet may be
30 appropriate in certain criminal cases of extraordinary public interest where information regarding
31 a case will be widely disseminated through the media. In such cases, posting of selected
32 nonconfidential court records, redacted where necessary to protect the privacy of the participants,
33 may provide more timely and accurate information regarding the court proceedings, and may
34 relieve substantial burdens on court staff in responding to individual requests for documents and
35 information. Thus, under subdivision (e), if the presiding judge makes individualized
36 determinations in a specific case, certain records in criminal cases may be made available over
37 the Internet.

38
39 **Subdivisions (f) and (g).** These subdivisions limit electronic access to records (other than the
40 register, calendars, or indexes) to a case-by-case basis and prohibit bulk distribution of those
41 records. These limitations are based on the qualitative difference between obtaining information
42 from a specific case file and obtaining bulk information that may be manipulated to compile
43 personal information culled from any document, paper, or exhibit filed in a lawsuit. This type of

1 aggregate information may be exploited for commercial or other purposes unrelated to the
2 operations of the courts, at the expense of privacy rights of individuals.

3
4 Courts must send a copy of the order permitting remote ~~electronic~~ access in extraordinary
5 criminal cases to: Criminal Justice Services, Judicial Council of California, 455 Golden Gate
6 Avenue, San Francisco, CA 94102-3688.

7
8 **Rules 2.504–2.507 * * ***

9
10 **Article 3. Remote Access by a Party, Party’s Designee, Party’s Attorney, Court-**
11 **Appointed Person, or Authorized Person Working in a Legal Organization or**
12 **Qualified Legal Services Project**

13
14 **Rule 2.515. Application and scope**

15
16 **(a) No limitation on access to electronic records available through article 2**

17
18 The rules in this article do not limit remote access to electronic records available
19 under article 2. These rules govern access to electronic records where remote
20 access by the public is not allowed.

21
22 **(b) Who may access**

23
24 The rules in this article apply to remote access to electronic records by:

- 25
26 (1) A person who is a party;
27
28 (2) A designee of a person who is a party,
29
30 (3) A party’s attorney;
31
32 (4) An authorized person working in the same legal organization as a party’s
33 attorney;
34
35 (5) An authorized person working in a qualified legal services project providing
36 brief legal services; and
37
38 (6) A court-appointed person.

39
40 **Advisory Committee Comment**

41
42 Article 2 allows remote access in most civil cases, and the rules in article 3 are not intended to
43 limit that access. Rather, the article 3 rules allow broader remote access—by parties, parties’

1 designees, parties' attorneys, authorized persons working in legal organizations, authorized
2 persons working in a qualified legal services project providing brief services, and court-appointed
3 persons—to those electronic records where remote access by the public is not allowed.

4
5 Under the rules in article 3, a party, a party's attorney, an authorized person working in the same
6 legal organization as a party's attorney, or a person appointed by the court in the proceeding
7 basically has the same level of access to electronic records remotely that they would have if they
8 were to seek to inspect the records in person at the courthouse. Thus, if they are legally entitled to
9 inspect certain records at the courthouse, they could view the same records remotely; on the other
10 hand, if they are restricted from inspecting certain court records at the courthouse (for example,
11 because the records are confidential or sealed), they would not be permitted to view the records
12 remotely. In some types of cases, such as unlimited civil cases, the access available to parties and
13 their attorneys is generally similar to the public's but in other types of cases, such as juvenile
14 cases, it is much more extensive (see Cal. Rules of Court, rule 5.552).

15
16 For authorized persons working in a qualified legal services program, the rule contemplates
17 services offered in high-volume environments on an ad hoc basis. There are some limitations on
18 access under the rule for qualified legal services projects. When an attorney at a qualified legal
19 services project becomes a party's attorney and offers services beyond the scope contemplated
20 under this rule, the access rules for a party's attorney would apply.

21 22 **Rule 2.516. Remote access to extent feasible**

23
24 To the extent feasible, a court that maintains records in electronic form must provide
25 remote access to those records to the users described in rule 2.515, subject to the
26 conditions and limitations stated in this article and otherwise provided by law.

27 28 **Advisory Committee Comment**

29
30 This rule takes into account the limited resources currently available in some trial courts. Many
31 courts may not have the financial means, security resources, or technical capabilities necessary to
32 provide the full range of remote access to electronic records authorized by this article. When it is
33 more feasible and courts have had more experience with remote access, these rules may be
34 modified to further expand remote access.

35
36 This rule is not intended to prevent a court from moving forward with limited remote access
37 options outlined in this rule as such access becomes feasible. For example, if it were only feasible
38 for a court to provide remote access to parties who are persons, it could proceed to provide
39 remote access to those users only.

1 **Rule 2.517. Remote access by a party**

2
3 **(a) Remote access generally permitted**

4
5 A person may have remote access to electronic records in actions or proceedings in
6 which that person is a party.

7
8 **(b) Level of remote access**

9
10 (1) In any action or proceeding, a party may be provided remote access to the
11 same electronic records that he or she would be legally entitled to inspect at
12 the courthouse.

13
14 (2) This rule does not limit remote access to electronic records available under
15 article 2.

16
17 (3) This rule applies only to electronic records. A person is not entitled under
18 these rules to remote access to documents, information, data, or other
19 materials created or maintained by the courts that are not electronic records.
20

21 **Advisory Committee Comment**

22
23 Because this rule permits remote access only by a party who is a person (defined under rule 2.501
24 as a natural person), remote access would not apply to organizational parties, which would need
25 to gain remote access through the party's attorney rule or, for certain government entities with
26 respect to specified electronic records, the rules in article 4.

27
28 A party who is a person would need to have the legal capacity to agree to the terms and
29 conditions of a court's remote access user agreement before using a system of remote access. The
30 court could deny access or require additional information if the court knew the person seeking
31 access lacked legal capacity or appeared to lack capacity, e.g., if identity verification revealed the
32 person seeking access was a minor.

33
34 **Rule 2.518. Remote access by a party's designee**

35
36 **(a) Remote access generally permitted**

37
38 A person may designate other persons to have remote access to electronic records
39 in actions or proceedings in which that person is a party.
40

1 **(b) Level of remote access**

2
3 (1) Except for criminal electronic records, juvenile justice electronic records, and
4 child welfare electronic records, a party’s designee may have the same access to
5 a party’s electronic records that a member of the public would be entitled to if
6 he or she were to inspect the party’s court records at the courthouse. A party’s
7 designee is not permitted remote access to criminal electronic records, juvenile
8 justice electronic records, and child welfare electronic records.

9
10 (2) A party may limit the access to be afforded a designee to specific cases.

11
12 (3) A party may limit the access to be afforded a designee to a specific period of
13 time.

14
15 (4) A party may modify or revoke a designee’s level of access at any time.

16
17 **(c) Terms of access**

18
19 (1) A party’s designee may access electronic records only for the purpose of
20 assisting the party or the party’s attorney in the action or proceeding.

21
22 (2) Any distribution for sale of electronic records obtained remotely under the
23 rules in this article is strictly prohibited.

24
25 (3) All laws governing confidentiality and disclosure of court records apply to
26 the records obtained under this article.

27
28 (4) Party designees must comply with any other terms of remote access required
29 by the court.

30
31 (5) Failure to comply with these rules may result in the imposition of sanctions,
32 including termination of access.

33
34 **Advisory Committee Comment**

35
36 A party must be a natural person with the legal capacity to agree to the terms and conditions of a
37 user agreement with the court to authorize designees for remote access. Under rule 2.501, for
38 purposes of the rules, “persons” are natural persons. Accordingly, the party designee rule would
39 not apply to organizational parties, which would need to gain remote access through the party’s
40 attorney rule or, for certain government entities with respect to specified electronic records, the
41 rules in article 4.

1 **Rule 2.519. Remote access by a party's attorney**

2
3 **(a) Remote access generally permitted**

4
5 (1) A party's attorney may have remote access to electronic records in the party's
6 actions or proceedings under this rule or rule 2.518. If a party's attorney gains
7 remote access through rule 2.518, the requirements of rule 2.519 do not
8 apply.

9
10 (2) If a court notifies an attorney of the court's intention to appoint the attorney
11 to represent a party in a criminal, juvenile justice, child welfare, family law,
12 or probate proceeding, the court may grant remote access to that attorney
13 before an order of appointment is issued by the court.

14
15 **(b) Level of remote access**

16
17 A party's attorney may be provided remote access to the same electronic records in
18 the party's actions or proceedings that the party's attorney would be legally entitled
19 to view at the courthouse.

20
21 **(c) Terms of remote access for attorneys who are not the attorney of record in the**
22 **party's actions or proceedings in the trial court**

23
24 An attorney who represents a party, but who is not the party's attorney of record,
25 may remotely access the party's electronic records, provided that the attorney:

26
27 (1) Obtains the party's consent to remotely access the party's electronic records;
28 and

29
30 (2) Represents to the court in the remote access system that the attorney has
31 obtained the party's consent to remotely access the party's electronic records.

32
33 **(d) Terms of remote access for all attorneys accessing electronic records**

34
35 (1) A party's attorney may remotely access the electronic records only for the
36 purposes of assisting the party with the party's court matter.

37
38 (2) A party's attorney may not distribute for sale any electronic records obtained
39 remotely under the rules in this article. Such sale is strictly prohibited.

40
41 (3) A party's attorney must comply with any other terms of remote access
42 required by the court.

43

1 **(c) Level of remote access**

- 2
- 3 (1) Persons designated by a party’s attorney under subdivision (b) must be
4 provided access to the same electronic records as the party.
- 5
- 6 (2) Notwithstanding subdivision (b), when a court designates a legal organization
7 to represent parties in criminal, juvenile, family, or probate proceedings, the
8 court may grant remote access to a person working in the organization who
9 assigns cases to attorneys working in that legal organization.

10

11 **(d) Terms of remote access**

- 12
- 13 (1) Persons working in a legal organization may remotely access electronic
14 records only for purposes of assigning or assisting a party’s attorney.
- 15
- 16 (2) Any distribution for sale of electronic records obtained remotely under the
17 rules in this article is strictly prohibited.
- 18
- 19 (3) All laws governing confidentiality and disclosure of court records apply to
20 the records obtained under this article.
- 21
- 22 (4) Persons working in a legal organization must comply with any other terms of
23 remote access required by the court.
- 24
- 25 (5) Failure to comply with these rules may result in the imposition of sanctions,
26 including termination of access.

27

28 **Advisory Committee Comment**

29

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

32

33 **Rule 2.521. Remote access by a court-appointed person**

34

35 **(a) Remote access generally permitted**

- 36
- 37 (1) A court may grant a court-appointed person remote access to electronic
38 records in any action or proceeding in which the person has been appointed
39 by the court.
- 40
- 41 (2) Court-appointed persons include an attorney appointed to represent a minor
42 child under Family Code section 3150; a Court Appointed Special Advocate
43 volunteer in a juvenile proceeding; an attorney appointed under Probate Code

1 section 1470, 1471, or 1474; an investigator appointed under Probate Code
2 section 1454; a probate referee designated under Probate Code section 8920;
3 a fiduciary, as defined in Probate Code section 39; an attorney appointed
4 under Welfare and Institutions Code section 5365; or a guardian ad litem
5 appointed under Code of Civil Procedure section 372 or Probate Code section
6 1003.

7
8 **(b) Level of remote access**

9
10 A court-appointed person may be provided with the same level of remote access to
11 electronic records as the court-appointed person would be legally entitled to if he or
12 she were to appear at the courthouse to inspect the court records.

13
14 **(c) Terms of remote access**

- 15
16 (1) A court-appointed person may remotely access electronic records only for
17 purposes of fulfilling the responsibilities for which he or she was appointed.
18
19 (2) Any distribution for sale of electronic records obtained remotely under the
20 rules in this article is strictly prohibited.
21
22 (3) All laws governing confidentiality and disclosure of court records apply to
23 the records obtained under this article.
24
25 (4) A court-appointed person must comply with any other terms of remote access
26 required by the court.
27
28 (5) Failure to comply with these rules may result in the imposition of sanctions,
29 including termination of access.
30

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

33
34 **(a) Application and scope**

- 35
36 (1) This rule applies to qualified legal services projects as defined in section
37 6213(a) of the Business and Professions Code.
38
39 (2) “Working in a qualified legal services project” under this rule includes
40 attorneys, employees, and volunteers.
41

1 (3) This rule does not apply to a person working in or otherwise associated with
2 a qualified legal services project who gains remote access to court records as
3 a party's designee under rule 2.518.
4

5 **(b) Designation and certification**
6

7 (1) A qualified legal services project may designate persons working in the
8 qualified legal services project who provide brief legal services, as defined in
9 article 1, to have remote access.
10

11 (2) The qualified legal services project must certify that the authorized persons
12 work in their organization.
13

14 **(c) Level of remote access**
15

16 Authorized persons may be provided remote access to the same electronic records
17 that the authorized person would be legally entitled to inspect at the courthouse.
18

19 **(d) Terms of remote access**
20

21 (1) Qualified legal services projects must obtain the party's consent to remotely
22 access the party's electronic records.
23

24 (2) Authorized persons must represent to the court in the remote access system
25 that the qualified legal services project has obtained the party's consent to
26 remotely access the party's electronic records.
27

28 (3) Qualified legal services projects providing services under this rule may
29 remotely access electronic records only to provide brief legal services.
30

31 (4) Any distribution for sale of electronic records obtained under the rules in this
32 article is strictly prohibited.
33

34 (5) All laws governing confidentiality and disclosure of court records apply to
35 electronic records obtained under this article.
36

37 (6) Qualified legal services projects must comply with any other terms of remote
38 access required by the court.
39

40 (7) Failure to comply with these rules may result in the imposition of sanctions,
41 including termination of access.
42

43 **Advisory Committee Comment**

1
2 The rule does not prescribe any particular method for capturing the designation and certification
3 of persons working in a qualified legal services project. Courts and qualified legal services
4 projects have flexibility to determine what method would work both for both entities. Examples
5 include: the information could be captured in a remote access system if an organizational-level
6 account could be established, or the information could be captured in a written agreement
7 between the court and the qualified legal services project.

8
9 The rule does not prescribe any particular method for a qualified legal services project to
10 document consent it obtained to access a person’s electronic records. Qualified legal services
11 projects have flexibility to adapt the requirement to their regular processes for making records.
12 Examples include: the qualified legal services project could obtain a signed consent form for its
13 records, could obtain consent over the phone and make an entry to that effect in its records, or the
14 court and qualified legal services project could enter an agreement to describe how consent will
15 be obtained and recorded.

16
17 **Rule 2.523. Identity verification, identity management, and user access**

18
19 **(a) Identity verification required**

20
21 Except for remote access provided to a party’s designee under rule 2.518, before
22 allowing a person who is eligible under the rules in article 3 to have remote access
23 to electronic records, a court must verify the identity of the person seeking access.

24
25 **(b) Responsibilities of the court**

26
27 A court that allows persons eligible under the rules in article 3 to have remote
28 access to electronic records must have an identity proofing solution that verifies the
29 identity of, and provides a unique credential to, each person who is permitted
30 remote access to the electronic records. The court may authorize remote access by a
31 person only if that person’s identity has been verified, the person accesses records
32 using the credential provided to that individual, and the person complies with the
33 terms and conditions of access, as prescribed by the court.

34
35 **(c) Responsibilities of persons accessing records**

36
37 A person eligible to be given remote access to electronic records under the rules in
38 article 3 may be given such access only if that person:

- 39
40 (1) Provides the court with all information it directs in order to identify the
41 person to be a user;
42

1
2 **(b) Vendor contracts and statewide master agreements**

3
4 A court may enter into a contract with a vendor to provide secure access and
5 encryption services. Alternatively, if a statewide master agreement is available for
6 secure access and encryption services, courts may use that master agreement.

7
8 **Advisory Committee Comment**

9
10 This rule describes security and encryption requirements; levels of access are provided for in
11 rules 2.517–2.522.

12
13 **Rule 2.525. Searches and access to electronic records in search results**

14
15 **(a) Searches**

16
17 A user authorized under this article to remotely access a party’s electronic records
18 may search for the records by case number or case caption.

19
20 **(b) Access to electronic records in search results**

21
22 A court providing remote access to electronic records under this article must ensure
23 that authorized users are able to access the electronic records only at the levels
24 provided in this article.

25
26 **(c) Unauthorized access**

27
28 If a user gains access to an electronic record that the user is not authorized to access
29 under this article, the user must:

- 30
31 (1) Report the unauthorized access to the court as directed by the court for that
32 purpose;
33
34 (2) Destroy all copies, in any form, of the record; and
35
36 (3) Delete from the user’s browser history all information that identifies the
37 record.
38

1 **Rule 2.526. Audit trails**

2
3 **(a) Ability to generate audit trails**

4
5 The court should have the ability to generate an audit trail that contains one or more
6 of the following elements: identifies each remotely accessed record, when an
7 electronic record was remotely accessed, who remotely accessed the electronic
8 record, and under whose authority the user gained access to the electronic record.

9
10 **(b) Limited audit trails available to authorized users**

11
12 (1) A court providing remote access to electronic records under this article
13 should make limited audit trails available to authorized users under this
14 article.

15
16 (2) A limited audit trail should show the user who remotely accessed electronic
17 records in a particular case but must not show which specific electronic
18 records were accessed.

19
20 **Advisory Committee Comment**

21
22 The audit trail is a tool to assist the courts and users in identifying and investigating any potential
23 issues or misuse of remote access. The user’s view of the audit trail is limited to protect sensitive
24 information.

25
26 While rule 2.526 is currently not mandatory to facilitate the use of existing remote access
27 systems, the committee expects the rule will become mandatory in the future.

28
29 **Rule 2.527. Additional conditions of access**

30
31 To the extent consistent with these rules and other applicable law, a court must
32 impose reasonable conditions on remote access to preserve the integrity of its
33 records, prevent the unauthorized use of information, and limit possible legal
34 liability. The court may choose to require each user to submit a signed, written
35 agreement enumerating those conditions before it permits that user to remotely
36 access electronic records. The agreements may define the terms of access, provide
37 for compliance audits, specify the scope of liability, and provide for the imposition
38 of sanctions for misuse up to and including termination of remote access.

1 **Rule 2.528. Termination of remote access**

2
3 **(a) Remote access is a privilege**

4
5 Remote access to electronic records under this article is a privilege and not a right.

6
7 **(b) Termination by court**

8
9 A court that provides remote access may, at any time and for any reason, terminate
10 the permission granted to any person eligible under the rules in article 3 to remotely
11 access electronic records.

12
13 **Article 4. Remote Access by Government Entities**

14
15 **Rule 2.540. Application and scope**

16
17 **(a) Applicability to government entities**

18
19 The rules in this article provide for remote access to electronic records by
20 government entities described in subdivision (b) below. The access allowed under
21 these rules is in addition to any access these entities or authorized persons working
22 for such entities may have under the rules in articles 2–3.

23
24 **(b) Level of remote access**

25
26 **(1) A court may provide authorized persons from government entities with**
27 **remote access to electronic records as follows:**

28
29 **(A) Office of the Attorney General: criminal electronic records and juvenile**
30 **justice electronic records.**

31
32 **(B) California Department of Child Support Services: family electronic**
33 **records, child welfare electronic records, and parentage electronic**
34 **records.**

35
36 **(C) Office of a district attorney: criminal electronic records and juvenile**
37 **justice electronic records.**

38
39 **(D) Office of a public defender: criminal electronic records and juvenile**
40 **justice electronic records.**

41

- 1 (E) Office of a county counsel: criminal electronic records, mental health
2 electronic records, child welfare electronic records, and probate
3 electronic records.
4
- 5 (F) Office of a city attorney: criminal electronic records, juvenile justice
6 electronic records, and child welfare electronic records.
7
- 8 (G) County department of probation: criminal electronic records, juvenile
9 justice electronic records, and child welfare electronic records.
10
- 11 (H) County sheriff’s department: criminal electronic records and juvenile
12 justice electronic records.
13
- 14 (I) Local police department: criminal electronic records and juvenile
15 justice electronic records.
16
- 17 (J) Local child support agency: family electronic records, child welfare
18 electronic records, and parentage electronic records.
19
- 20 (K) County child welfare agency: child welfare electronic records.
21
- 22 (L) County public guardian: criminal electronic records, mental health
23 electronic records, and probate electronic records.
24
- 25 (M) County agency designated by the board of supervisors to provide
26 conservatorship investigation under chapter 3 of the Lanterman-Petris-
27 Short Act (Welf. & Inst. Code, §§ 5350–5372): criminal electronic
28 records, mental health electronic records, and probate electronic
29 records.
30
- 31 (N) Federally recognized Indian tribe (including any reservation,
32 department, subdivision, or court of the tribe) with concurrent
33 jurisdiction: child welfare electronic records, family electronic records,
34 juvenile justice electronic records, and probate electronic records.
35
- 36 (O) For good cause, a court may grant remote access to electronic records
37 in particular case types to government entities beyond those listed in
38 (b)(1)(A)–(N). For purposes of this rule, “good cause” means that the
39 government entity requires access to the electronic records in order to
40 adequately perform its statutory duties or fulfill its responsibilities in
41 litigation.
42

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

3
4 (2) Subject to (b)(1), the court may provide a government entity with the same
5 level of remote access to electronic records as the government entity would
6 be legally entitled to if a person working for the government entity were to
7 appear at the courthouse to inspect court records in that case type. If a court
8 record is confidential by law or sealed by court order and a person working
9 for the government entity would not be legally entitled to inspect the court
10 record at the courthouse, the court may not provide the government entity
11 with remote access to the confidential or sealed electronic record.

12
13 (3) This rule applies only to electronic records. A government entity is not
14 entitled under these rules to remote access to any documents, information,
15 data, or other types of materials created or maintained by the courts that are
16 not electronic records.

17
18 **(c) Terms of remote access**

19
20 (1) Government entities may remotely access electronic records only to perform
21 official duties and for legitimate governmental purposes.

22
23 (2) Any distribution for sale of electronic records obtained remotely under the
24 rules in this article is strictly prohibited.

25
26 (3) All laws governing confidentiality and disclosure of court records apply to
27 electronic records obtained under this article.

28
29 (4) Government entities must comply with any other terms of remote access
30 required by the court.

31
32 (5) Failure to comply with these requirements may result in the imposition of
33 sanctions, including termination of access.

34
35 **Advisory Committee Comment**

36
37 The rule does not restrict courts to providing remote access only to local government entities in
38 the same county in which the court is situated. For example, a court in one county could allow
39 remote access to electronic records by a local child support agency in a different county.

40
41 **Subdivision (b)(3).** On the applicability of the rules on remote access only to electronic records,
42 see the advisory committee comment to rule 2.501.

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

2
3 **(a) Identity verification required**

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

8
9 **(b) Responsibilities of the courts**

10
11 A court that allows persons eligible under the rules in article 4 to have remote
12 access to electronic records must have an identity proofing solution that verifies the
13 identity of, and provides a unique credential to, each person who is permitted
14 remote access to the electronic records. The court may authorize remote access by a
15 person only if that person’s identity has been verified, the person accesses records
16 using the name and password provided to that individual, and the person complies
17 with the terms and conditions of access, as prescribed by the court.

18
19 **(c) Responsibilities of persons accessing records**

20
21 A person eligible to remotely access electronic records under the rules in article 4
22 may be given such access only if that person:

- 23
24 (1) Provides the court with all information it needs to identify the person to be a
25 user;
26
27 (2) Consents to all conditions for remote access required by article 4 and the
28 court; and
29
30 (3) Is authorized by the court to have remote access to electronic records.

31
32 **(d) Responsibilities of government entities**

- 33
34 (1) If a person is accessing electronic records on behalf of a government entity,
35 the government entity must approve granting access to that person, verify the
36 person’s identity, and provide the court with all the information it needs to
37 authorize that person to have access to electronic records.
38
39 (2) If a person accessing electronic records on behalf of a government entity
40 leaves his or her position or for any other reason is no longer entitled to
41 access, the government entity must immediately notify the court so that it can
42 terminate the person’s access.

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

3
4 A court may enter into a contract with a vendor to provide identity verification,
5 identity management, or user access services. Alternatively, if a statewide identity
6 verification, identity management, or access management system or a statewide
7 master agreement for such systems is available, courts may use those for identity
8 verification, identity management, and user access services.

9
10 **Rule 2.542. Security of confidential information**

11
12 **(a) Secure access and encryption required**

13
14 If any information in an electronic record that is confidential by law or sealed by
15 court order may lawfully be provided remotely to a government entity, any remote
16 access to the confidential information must be provided through a secure platform,
17 and any electronic transmission of the information must be encrypted.

18
19 **(b) Vendor contracts and statewide master agreements**

20
21 A court may enter into a contract with a vendor to provide secure access and
22 encryption services. Alternatively, if a statewide master agreement is available for
23 secure access and encryption services, courts may use that master agreement.

24
25 **Rule 2.543. Audit trails**

26
27 **(a) Ability to generate audit trails**

28
29 The court should have the ability to generate an audit trail that contains one or more
30 of the following elements: identifies each remotely accessed record, when an
31 electronic record was remotely accessed, who remotely accessed the electronic
32 record, and under whose authority the user gained access to the electronic record.

33
34 **(b) Audit trails available to government entity**

35
36 (1) A court providing remote access to electronic records under this article
37 should make limited audit trails available to authorized users of the
38 government entity.

39
40 (2) A limited audit trail should show the user who remotely accessed electronic
41 records in a particular case, but must not show which specific electronic
42 records were accessed.

1
2 Advisory Committee Comment
3

4 The audit trail is a tool to assist the courts and users in identifying and investigating any potential
5 issues or misuse of remote access. The user's view of the audit trail is limited to protect sensitive
6 information.
7

8 While rule 2.543 is currently not mandatory to facilitate the use of existing remote access
9 systems, the committee expects the rule will become mandatory in the future.
10

11 **Rule 2.544. Additional conditions of access**
12

13 To the extent consistent with these rules and other applicable law, a court must impose
14 reasonable conditions on remote access to preserve the integrity of its records, prevent the
15 unauthorized use of information, and protect itself from liability. The court may choose
16 to require each user to submit a signed, written agreement enumerating those conditions
17 before it permits that user to access electronic records remotely. The agreements may
18 define the terms of access, provide for compliance audits, specify the scope of liability,
19 and provide for sanctions for misuse up to and including termination of remote access.
20

21 **Rule 2.545. Termination of remote access**
22

23 **(a) Remote access is a privilege**
24

25 Remote access under this article is a privilege and not a right.
26

27 **(b) Termination by court**
28

29 A court that provides remote access may terminate the permission granted to any
30 person or entity eligible under the rules in article 4 to remotely access electronic
31 records at any time for any reason.
32

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
1	<p>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</p>	AM	<p>Thank you for this opportunity to provide formal Comment to Judicial Council proposal SPR18-37, titled "<u>Technology: Remote Access to Electronic Records</u>". 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.</p>	<p>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.</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>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: <u>Article 4. Remote Access by Government Entities, Rule 2.54o(b)</u>, which provides:</p> <p><u>(b) Level of remote access</u></p> <p><u>(1) A court may provide authorized persons from government entities with remote access to electronic records as follows:</u></p> <p>...</p> <p><u>(B) California Department of Child Support Services: family electronic records, child welfare electronic records, and parentage electronic records.</u> [Emphasis added]</p> <p>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</p>	

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>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.</p> <p>However, the CSDA suggests the following language as to subsection (b)(1):</p> <p><u>(1) A court shall provide authorized persons from government entities with remote access to electronic records as follows:</u></p> <p>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</p>	

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>electronic records specified in subdivision (b)(1)(B).</p> <p>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.</p> <p>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</p>	

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>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".</p> <p>The CSDA appreciates the Judicial Council's consideration of this comment and appreciates the opportunity to provide input in this process.</p>	
2	<p>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</p>	AM	<p>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.</p> <p><u>Rule 2.540</u></p>	<p>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.</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>The Department supports the adoption of this rule for the following reasons:</p> <ol style="list-style-type: none"> 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. <p>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,</p>	<p>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.</p> <p>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</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>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.</p> <p>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 vital [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 ongoing in-state court</p>	<p>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.</p> <p>The committee declines to include non-exhaustive list of authorities on “parentage” as it is unnecessary.</p> <p>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.</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>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.</p> <p>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 ameliorate this risk, the Department respectfully requests that the JCC consider amending the child support provisions of Rule 2.540(b)(1) in two ways.</p> <p>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</p>	

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>be.treated differently. This problem could be avoided by combining (b)(1)(B) an (b)(1)(J) into a single exception, . as follows:</p> <p>(b)(1)(B) California Department of Child Support Services <i>and local child support agencies</i>: family electronic records, child welfare electronic records, and parentage electronic records.</p> <p>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:</p>	

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>(b)(1)(B) California Department of Child Support Services <i>and local child support agencies</i>: family electronic records, child welfare electronic records, and parentage electronic records. <i>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.</i></p> <p>The Department is also concerned that the rule, as drafted, might have other unintended</p>	

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>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</p>	

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>word "agency" be changed to "agencies" as stated above.</p> <p>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.</p> <p>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</p>	

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>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:</p> <p style="padding-left: 40px;">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.</p>	
3	<p>California Lawyers Association, by The Executive Committee of the Trust and Estates Section of CLA 180 Howard Street, Suite 410 San Francisco, CA 94105</p>	AM	<p>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,</p>	<p>The committee appreciates the comments. The suggested language provides clarity and will be added to the rule.</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
	<p><u>TEXCOM</u></p> <p>Ellen McKissock Hopkins & Carley Tel: 408-286-9800 E-mail: emckissock@hopkinscarley.com</p> <p><u>California Lawyers Association</u></p> <p>Saul Bercovitch Director of Governmental Affairs California Lawyers Association Tel: 415-795-7326 E-mail: saul.bercovitch@calawyers.org</p>		<p>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 <i>is not</i> 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:</p> <p>Rule 2.515 Application and scope</p>	

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>(a) No limitation on access to electronic records available through article 2</p> <p>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.</p> <p>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.</p>	
4	<p>Timothy Cassidy-Curtis 4467 Lakewood Blvd. Lakewood, CA 90712 Email: tcassidycurtis@roadrunner.com</p>	AM	<p>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,</p>	<p>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).</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

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

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>make an order (with, possibly, some payment to defray Court's costs), with a certified document mailed to us.</p> <p>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.</p>	
5	<p>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</p>	N	<p>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</p>	<p>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.</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>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 forth, it appears that the rules for a party’s or attorneys access are more constricted 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.</p> <p>Rule 2.501(b) appears to grant individual trial courts rights to further define and limit access which defeats the very purpose of these proposed “uniform” rules.</p>	<p>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.</p> <p>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.</p> <p>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.</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>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.</p> <p>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.</p> <p>The entirety of Article 4 has the same problems as Article 3 and suffers again from being unnecessary for these purposes.</p>	
6	<p>Superior Court of California, County of Orange By Cynthia Beltrán, Administrative Analyst Family Law and Juvenile Court</p>	NI	<p>What would the implementation requirements be for courts? <i>This is dependent upon whether or not courts have existing applications that allow remote access.</i></p>	<p>The committee appreciates the responses to the request for specific comments and they are helpful providing needed information to the committee.</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
	<p>Tel: 657-622-6128 E-mail: cbeltran@occourts.org</p>		<p>What implementation guidance, if any, would courts find helpful? <i>A quick reference Should proposed rule 2.518 be limited to certain case types?</i> <i>Yes, the rule should be clear that it does not apply to juvenile justice and dependency case types.</i></p> <p>Would an alternative term like “preliminary legal services” be more clear? <i>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?</i></p> <p>Is the term “legal organization” and its definition clear or necessary? <i>Yes, it is clear and necessary.</i></p>	<p>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.</p> <p>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.</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>Would referring to persons “working at the direction of an attorney” be sufficient? <i>No, that is too broad of a definition.</i></p> <p>Is “concurrent jurisdiction” the best way to describe such cases or would different phrasing be more accurate? <i>Concurrent jurisdiction should be defined within the rule itself.</i></p> <p>Is the standard for “good cause” in proposed rule 2.540(b)(1)(O) clear? <i>Yes</i></p> <p>Would the proposal provide cost savings? <i>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.</i></p>	<p>The comments on costs will be included with the Judicial Council report.</p> <p>The committee will add an advisory committee comment explaining the purpose of the audit trail.</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p><i>Managing user ID's and password control should also be considered. guide for courts to reference when developing remote access applications would be helpful.</i></p> <p>Would providing limited audit trails to users under rule 2.256 present a significant operational challenge to the court?</p> <p><i>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.</i></p>	

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
7	Superior Court of California, County of Orange, West Justice Center By Albert De La Isla, Principal Analyst IMPACT Team – Criminal Operations Tel: 657-622-5919 Email: adelaisla@occourts.org	NI	For courts that already provide electronic remote access to defense and prosecutors / law enforcement, would we have to go back and re-certify each access as well as have them sign user forms?	To the extent remote access is already being provided consistent with the rules, there is no need to re-do any certifications or user agreements. If remote access is provided that is not compliant with the rules then the courts should take necessary steps to become compliant. Note that the rules do not prescribe any particular method for identity verification or capturing consent. This could be done through agreements between the government entities and the court (e.g., the government entities will have almost certainly verified the identities of their own employees and can confirm that is authorized users are who they say they are).
8	Superior Court of Placer County By Jake Chatters Court Executive Officer 10820 Justice Center Drive, Roseville, CA 95678 P. O. Box 619072, Roseville, CA 95661 Tel: 916-408-6186	AM	The Placer Superior court appreciates the opportunity to comment on the proposed California Rules of Court 2.515-2.528 and 2.540-2.545 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.

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
	Fax: 916-408-6188		<p>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.</p> <p>Thank you again for the opportunity to comment.</p>	
9	<p>Superior Court of San Bernardino County By Executive Office ExecutiveOffice@sb-court.org</p>	NI	<p>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</p>	<p>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.</p> <p>Regarding the level of remote access, the committee assumes the comment is in reference to rule</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>and provide clear authority to the courts.</p> <p>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.)</p> <p>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).</p>	<p>2.540(b), which is the only rule that mentions public defenders in particular. That rule 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.</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>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 Litem that are appointed in juvenile court matters.</p>	
10	<p>Superior Court of California, County of San Diego By Mike Roddy, Executive Officer 1100 Union Street San Diego, CA 92101</p>	AM	<p>Q: Does the proposal appropriately address the stated purpose? Yes.</p> <p>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</p>	<p>The committee appreciates the responses to the request for specific comments. They are helpful and insightful information for committee to consider.</p> <p>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.</p> <p>The comments on costs and implementation will be included with the Judicial Council report.</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>someone who is over 18 years of age but under a Conservatorship?</p> <p>Q Should proposed rule 2.518 be limited to certain case types? No.</p> <p>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.</p>	<p>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.</p> <p>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.</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>Q Is the term “legal organization” and its definition clear or necessary? The proposed “legal organization” is clear.</p> <p>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.</p> <p>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</p>	

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>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.</p> <p>Q Is the standard for “good cause” in proposed rule 2.540(b)(1)(O) clear? Yes.</p> <p>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</p>	

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>scheme be clearer? The included language is clear and reduces the need for the user to refer to additional rules.</p> <p>Q: Would the proposal provide cost savings? No.</p> <p>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:</p> <p>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</p>	

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>example, do we need to restrict access from specific networks.</p> <p>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.</p> <p>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).</p> <p>4. Training. Tip sheets will need to be prepared for the users.</p> <p>5. Legal. There needs to be some kind of MOU with the remote user\justice partner.</p> <p>Q: What implementation guidance, if any, would courts find helpful? A governance and best practice checklist for implementing remote access.</p> <p>Q: The audit trail requirements are intended to provide both the courts and users with a mechanism to</p>	

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>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.</p> <p><u>General Comments:</u></p> <p>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</p> <p>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.</p>	
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

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
	<p>Records Manager 540 E Main Street Stockton CA 95202 Tel: 209-992-5221 eochoa@sjcourts.org</p>		<ul style="list-style-type: none"> 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>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.</i> Should proposed rule 2.518 be limited to certain case types? <i>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</i> 	<p>the committee’s recommendation to the council.</p> <p>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.</p> <p>Comments on the costs and implementation will be included with the Judicial Council report.</p> <p>Regarding the audit trail, the committee declines to add “good cause” language. The committee has instead made the audit trail permissive rather than mandatory.</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>will be front and center rather than the right to protect information.</p> <ul style="list-style-type: none"> • 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. <p>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”</p>	

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>rather than “preliminary” makes it clearer as to their involvement in the case.</p> <ul style="list-style-type: none"> • 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 	

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>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”.</p> <ul style="list-style-type: none"> • 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 	

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>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.</p> <p>Would another organizational scheme be clearer? No additional comment.</p> <ul style="list-style-type: none"> • 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	Committee Response
			<p>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.</p> <ul style="list-style-type: none"> • 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? <p>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:</p> <ul style="list-style-type: none"> • Set up, testing, training, and implementation of an additional program because our current case 	

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>management system is not set up to handle the identity and audit trails required in the amendment.</p> <ul style="list-style-type: none"> • 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	Committee Response
			<p>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?</p> <p>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.</p> <p>If so, is there a more feasible alternative?</p> <p>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.</p>	
12	<p>TCPJAC/CEAC Joint Rules Subcommittee (JRS) By Corey Rada, Senior Analyst Judicial Council and Trial Court Leadership Leadership Services Division</p>	AM	<p>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</p>	<p>The committee appreciates the comments. The comments on impacts on case management systems, workload, and security will be included with the Judicial Council report.</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
	<p>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</p>		<p>Court Executives Advisory Committee (CEAC).</p> <p>SPR18-37: Recommended JTS Position: Agree with proposed changes if modified.</p> <p>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:</p> <ul style="list-style-type: none"> 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 	<p>Regarding rule 2.502(4), the suggested modification is clearer and the committee recommends it.</p> <p>Regarding rule 2.503(b)(2), the suggested modification will be made as a technical correction.</p> <p>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.</p> <p>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</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>costs, and complicate the access rules in a way that may result in confusion for the public.</p> <ul style="list-style-type: none"> • 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. <p><i>Suggested Modifications:</i></p> <ul style="list-style-type: none"> • Rule 2.502 Definitions <ul style="list-style-type: none"> ○ Modify the definition of “court case information” to use more natural language to reduce confusion. A possible definition might be: <p>“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</p>	<p>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.</p> <p>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</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>the action and is not part of the official court record for the case or cases.</p> <ul style="list-style-type: none"> • Rule 2.503(b)(2) <ul style="list-style-type: none"> ○ “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 <ul style="list-style-type: none"> ○ 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: <i>Courts should provide remote access to the</i> 	<p>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.</p> <p>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.</p> <p>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</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p><i>greatest extent feasible, even in situations where all access outlined in these rules is not feasible.</i></p> <p>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.”</p> <ul style="list-style-type: none"> • Rule 2.518 Remote access by a party’s designee <p>TCPJAC and CEAC strongly encourages ITAC to amend this provision. TCPJAC/CEAC offers the following additional comments:</p> <ul style="list-style-type: none"> ▪ 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, 	<p>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.</p> <p>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</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>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.</p> <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> ○ This rule presents a significant security risk to court data and could add an additional burden on the court. <p>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</p>	<p>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.</p> <p>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</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>court would verify the identity of the attorney who is not of record in this process.</p> <p>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</p>	<p>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.</p> <p>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.</p> <p>Regarding 2.520, the committee agrees to add the advisory committee comment. The rules do not require any specific process.</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>ITAC to amend this provision and offer the following additional comments:</p> <ul style="list-style-type: none"> ▪ 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. <ul style="list-style-type: none"> • Rule 2.520 Remote access by persons working in the same legal organization as a party’s attorney. <ul style="list-style-type: none"> ○ We suggest adding an Advisory Committee Comment that the designation and certification outlined in (b) need only be done 	<p>Certifying at one time and having that time be when an attorney establishes a remote access account is a logical and practical option.</p> <p>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.</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>once and can be done at the time the attorney establishes their remote account with the court.</p> <ul style="list-style-type: none"> • 2.522 Remote access by persons working in a qualified legal services project providing brief legal services. <ul style="list-style-type: none"> ○ 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: <ul style="list-style-type: none"> ▪ 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 	<p>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.</p> <p>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.</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>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.</p> <ul style="list-style-type: none"> ▪ 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. <p>• Rule 2.523 – Identity</p>	<p>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.</p> <p>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.</p> <p>Regarding rule 2.523, the committee agrees 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 (attorneys who have made an</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>verification, identity management, and user access</p> <ul style="list-style-type: none"> ○ 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. <p>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</p>	<p>appearance, and attorneys who are undisclosed). Rule 2.522 will have persons unknown to the court. The identity verification process is meant to provide a way for unknown persons to be known and to verify that known persons are who they say they are. The rule is meant to be flexible in how a court verifies identities and it could be done by the court or through agreements with third parties, e.g., an agreement with a company that provides identity verification services, or an agreement with a qualified legal services project that the project is required to verify the identities and provide that verification to the court (it is likely that with respect to its own employees, a qualified legal services project would have already done its due diligent to verify that a person is who they say they are).</p> <p>In addition, rule 2.523(c) puts the onus on the person seeking remote access to provide the court with all information it directs in order to identify the person. The court is not</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>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.</p> <ul style="list-style-type: none"> ○ 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. <ul style="list-style-type: none"> ○ We suggest adding an Advisory Committee Comment that specifies that data transmitted via HTTPS complies with the encryption requirement. • Rule 2.526 Audit trails <ul style="list-style-type: none"> ○ 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 	<p>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.</p> <p>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 organization. The committee will</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	Committee Response
			<p>retain this section, we recommend it be modified as follows: <i>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.</i></p> <p>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</p>	<p>add an advisory committee comment to clarify that (d) can satisfy (a).</p> <p>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.</p> <p>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 improved. The committee agrees</p>

ITC SPR18-37

Technology: Remote Access to Electronic Records

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

#	Commentator	Position	Comment	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.	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 personally approve of these changes.	The committee appreciates the support.