



JUDICIAL COUNCIL
OF CALIFORNIA

TECHNOLOGY COMMITTEE

www.courts.ca.gov/jctc.htm
jctc@jud.ca.gov

JUDICIAL COUNCIL TECHNOLOGY COMMITTEE

Open to the Public (Cal. Rules of Court, rule 10.75(c)(1))
THIS MEETING WILL BE CONDUCTED BY TELECONFERENCE
THIS MEETING WILL BE RECORDED

Date: February 5, 2018
Time: 12:00 noon - 1:00 p.m.
Public Call-in Number: 1-877-820-7831 Passcode: 3511860

Meeting materials will be posted on the advisory body web page on the California Courts website at least three business days before the meeting.

Agenda items are numbered for identification purposes only and will not necessarily be considered in the indicated order.

I. OPEN MEETING (CAL. RULES OF COURT, RULE 10.75(C)(1))

Call to Order and Roll Call

Approval of Minutes

Approve minutes of the January 8, 2018 meeting.

II. PUBLIC COMMENT (CAL. RULES OF COURT, RULE 10.75(K)(2))

Written Comment

In accordance with California Rules of Court, rule 10.75(k)(1), public comments about any agenda item must be submitted by February 2, 2018, 12:00 noon. Written comments should be e-mailed to jctc@jud.ca.gov or mailed or delivered to 455 Golden Gate Avenue, San Francisco, CA 94102, attention: Rica Abesa. Only written comments received by February 2, 2018, 12:00 noon will be provided to advisory body members prior to the start of the meeting.

III. DISCUSSION AND POSSIBLE ACTION ITEMS (ITEMS 1-7)

Item 1

Chair Report

Provide update on activities of or news from the Judicial Council, advisory bodies, courts, and/or other justice partners.

Presenter: Hon. Marsha G. Slough, Chair, Judicial Council Technology Committee

Item 2

Update/Report on Information Technology Advisory Committee (ITAC)

An update and report on ITAC will be provided; this will include the activities of the workstreams.

Presenter: Hon. Sheila F. Hanson, Chair, Information Technology Advisory Committee

Item 3

Update on V3 Case Management System

An update and report on the work to date on V3 court conversion projects since receiving the funding for civil case management system replacement.

Presenter: Ms. Kathy Fink, Manager, Judicial Council Information Technology

Item 4

Update on Sustain Justice Edition Case Management System

An update and report on the work related to the Sustain Justice Edition case management system.

Presenter: Mr. David Koon, Manager, Judicial Council Information Technology

Item 5

Modernization Project: Rules Proposal, Proposed Amendments to Title 2, Division 3, Chapter 2 (Action Requested)

Review proposed amendments to title 2, division 3, chapter 2 of the California Rules of Court for public comment. The proposed amendments respond to new requirements in Code of Civil Procedure section 1010.6, amend definitions in the rules, and ensure indigent filers are not required to have a payment mechanism to create an account with electronic filing service providers. Consider whether to recommend circulating proposed amendments for public comment.

Presenters: Hon. Peter J. Siggins, Chair, Rules and Policy Subcommittee; Mr. Patrick O'Donnell, Principal Managing Attorney, Judicial Council Legal Services; and Ms. Andrea L. Jaramillo, Attorney, Judicial Council Legal Services

Item 6

Modernization Project: Form Proposal, Withdrawal of Consent to Electronic Service (Action Requested)

Review proposed Judicial Council form EFS-006-CV, *Withdrawal of Consent to Electronic Service*. The purpose of the proposal is to comply with Code of Civil Procedure section 1010.6(a)(6), which requires the Judicial Council to create such a form by January 1, 2019. This is a joint proposal with the Civil and Small Claims Advisory Committee. Consider whether to recommend circulating proposed amendments for public comment.

Presenters: Hon. Peter J. Siggins, Chair, Rules and Policy Subcommittee; Mr. Patrick O'Donnell, Principal Managing Attorney, Judicial Council Legal Services; and Ms. Andrea L. Jaramillo, Attorney, Judicial Council Legal Services

Item 7

Remote Access for Government Entities, Parties, Attorneys Rules Proposal: Proposed Amendments to Title 2, Division 1, Chapter 2 of the California Rules of Court (Action Requested)

Review proposed amendments to Title 2, Division 1, Chapter 2 of the California Rules of Court. The proposal is designed to facilitate remote access to trial court records by state, local, and tribal government entities, parties, parties' attorneys, and court-appointed persons. Consider whether to recommend circulating proposed amendments for public comment.

Presenters: Hon. Peter J. Siggins, Chair, Rules and Policy Subcommittee; Mr. Patrick O'Donnell, Principal Managing Attorney, Judicial Council Legal Services; and Ms. Andrea L. Jaramillo, Attorney, Judicial Council Legal Services

A D J O U R N M E N T

Adjourn

The background features a large, faint, circular seal of the Judicial Council of Pennsylvania. The seal contains a central figure holding a scale and a sword, surrounded by the text "JUDICIAL COUNCIL OF PENNSYLVANIA" and the year "1926".

Judicial Council Technology Committee Open Meeting

February 5, 2018

Call to Order and Roll Call

- Welcome
- Open Meeting Script

*Hon. Marsha G. Slough, Chair, Judicial Council Technology
Committee*



JUDICIAL COUNCIL
OF CALIFORNIA

Chair Report

Hon. Marsha G. Slough



JUDICIAL COUNCIL
OF CALIFORNIA

Update: Information Technology Advisory Committee (ITAC)

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



JUDICIAL COUNCIL
OF CALIFORNIA

Update: V3 Case Management System

Ms. Kathy Fink, Manager, Judicial Council Information Technology



JUDICIAL COUNCIL
OF CALIFORNIA

Update: Sustain Justice System (SJE) Case Management System

Mr. David Koon, Manager, Judicial Council Information Technology



JUDICIAL COUNCIL
OF CALIFORNIA

Action: Modernization Project: Rules Proposal, Proposed Amendments to Title 2, Division 3, Chapter 2

Hon. Peter J. Siggins, Chair, Rules and Policy Subcommittee; Mr. Patrick O'Donnell, Principal Managing Attorney, Judicial Council Legal Services; and Ms. Andrea L. Jaramillo, Attorney, Judicial Council Legal Services



JUDICIAL COUNCIL
OF CALIFORNIA

Action: Modernization Project: Form Proposal, Withdrawal of Consent to Electronic Service

Hon. Peter J. Siggins, Chair, Rules and Policy Subcommittee; Mr. Patrick O'Donnell, Principal Managing Attorney, Judicial Council Legal Services; and Ms. Andrea L. Jaramillo, Attorney, Judicial Council Legal Services



JUDICIAL COUNCIL
OF CALIFORNIA

Action: Remote Access for Government Entities, Parties, Attorneys Rules Proposal: Proposed Amendments to Title 2, Division 1, Chapter 2 of the California Rules of Court

Hon. Peter J. Siggins, Chair, Rules and Policy Subcommittee; Mr. Patrick O'Donnell, Principal Managing Attorney, Judicial Council Legal Services; and Ms. Andrea L. Jaramillo, Attorney, Judicial Council Legal Services



JUDICIAL COUNCIL
OF CALIFORNIA

Adjourn

A//



JUDICIAL COUNCIL
OF CALIFORNIA



JUDICIAL COUNCIL OF CALIFORNIA

TECHNOLOGY COMMITTEE

www.courts.ca.gov/jctc.htm
jctc@jud.ca.gov

JUDICIAL COUNCIL TECHNOLOGY COMMITTEE

MINUTES OF OPEN MEETING

January 8, 2018

12:00 - 1:00 PM

Teleconference

Advisory Body Members Present: Hon. Marsha G. Slough, Chair; Hon. Gary Nadler, Vice-Chair; Mr. Jake Chatters; Hon. Ming W. Chin; Ms. Rachel W. Hill; Ms. Audra Ibarra; Hon. Shama H. Mesiwala; and Ms. Andrea K. Rohmann

Advisory Body Members Absent: Hon. Kyle S. Brodie

Liaison Members Present: Hon. Sheila F. Hanson

Others Present: Hon. Jack Lucky; Mr. Brian Cotta; Ms. Heather Pettit; Mr. Robert Oyung, Ms. Jessica Goldstein; Ms. Jamel Jones; Mr. Mark Dusman; Ms. Virginia Sanders-Hinds; Mr. Michael Derr; Ms. Kathy Fink; Ms. Donna Keating; Mr. John Yee; Ms. Daphne Light; and Mr. Zlatko Theodorovic

OPEN MEETING

Call to Order and Roll Call

The chair called the meeting to order, took roll call, and advised no public comments were received.

Approval of Minutes

The advisory body reviewed and approved the minutes of the December 11, 2017 meeting (with one abstention).

DISCUSSION AND ACTION ITEMS

Item 1

Chair Report

Update: Hon. Marsha Slough, Chair of the Judicial Council Technology Committee (JCTC), welcomed and thanked everyone for attending. Justice Slough reviewed the agenda for the meeting, as well as provided updates on recent meetings in which she and other members represented the JCTC or reported on the JCTC activities.

Item 2

Review of Information Technology Advisory Committee's (ITAC) Annual Agenda (Action Requested)

Update: Hon. Sheila F. Hanson, Chair of ITAC, reviewed ITAC's annual agenda with the committee.

Action: The committee discussed the activities of ITAC, asked questions, and approved the ITAC annual agenda allowing further technical amendments and other non-substantive revisions to be made at the discretion of the ITAC Chair and staff following formal approval, as needed.

Item 3

Disaster Recovery Framework Workstream – Final Deliverables (Action Requested)

Update: Mr. Brian Cotta, the workstream's executive co-sponsor and project manager, reviewed the workstream's final deliverables and decide whether to approve. Also, consider whether it is appropriate to recommend the deliverables to the Judicial Council for adoption. The deliverables include a Disaster Recovery Framework, Adaptable Disaster Recovery Plan, a "How to Guide," and budget change proposal (BCP) recommendations.

Action: The committee discussed the Disaster Recovery Framework final deliverables, asked questions, and approved the final deliverables allowing further technical amendments and other non-substantive revisions to be made at the discretion of the ITAC Chair and staff following formal approval, as needed.

Item 4

Next Generation Hosting Strategy Workstream – Final Deliverables (Action Requested)

Update: Ms. Heather Pettit, the workstream's project manager and court lead, reviewed the workstream's final deliverables and decide whether to approve. Also, consider whether it is appropriate to recommend the deliverables to the Judicial Council for adoption. The deliverables include a Next Generation Hosting Framework, recommendations, and budgeting/roadmapping spreadsheet tools.

Action: The committee discussed the Next Generation Hosting final deliverables, asked questions, and approved the final deliverables allowing further technical amendments and other non-substantive revisions to be made at the discretion of the ITAC Chair and staff following formal approval, as needed.

A D J O U R N M E N T

There being no further business, the meeting was adjourned.

INVITATION TO COMMENT

[ItC prefix as assigned]-__

Title	Action Requested
Technology: Rules Modernization Project	Review and submit comments by June 8, 2018
Proposed Rules, Forms, Standards, or Statutes	Proposed Effective Date
Amend Cal. Rules of Court, 2.250, 2.251, 2.255, and 2.257	January 1, 2019
Proposed by	Contact
Information Technology Advisory Committee	Andrea Jaramillo, 916-263-0991
Hon. Sheila F. Hanson, Chair	andrea.jaramillo@jud.ca.gov

Executive Summary and Origin

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

Background

New provisions of Code of Civil Procedure section 1010.6 require express consent for electronic service, which will require rule amendments and adoption of a form for withdrawal of consent. In addition, new provisions of Code of Civil Procedure 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 electronic filing service providers and courts.

The Proposal

The proposal would:

- Amend the definition of “document” in rule 2.250(b). The current wording can be read to mean that a document must be a filing. The proposed amendment removes this ambiguity by striking “filing” and replacing it with “writing” to clarify that a “document” is not necessarily a filing. The amendment was suggested by members of the public.

- Amend the definitions of “electronic service,” “electronic transmission,” and “electronic notification” in rule 2.250(b) to refer to the definitions in Code of Civil Procedure section 1010.6 rather than duplicate them. This is to avoid risk of the rules and Code of Civil Procedure differing in their definitions should the Legislature amend Code of Civil Procedure section 1010.6.
- Add a definition for “electronic filing manager.” The proposal includes amendments to rule 2.255 to include electronic filings managers. Accordingly, a definition of electronic filing manager was also added. The proposed definition is based on descriptions the Judicial Council used of electronic filing managers in a request for proposals in 2017.
- Add a definition for “self-represented” to rule 2.250(b) and exclude attorneys from the definition. Rules applicable to self-represented persons were intended to add protections for those without an attorney. For example, self-represented persons are exempt from mandatory electronic filing. Attorneys acting for themselves are not acting without an attorney. Accordingly, attorneys are excluded from the definition of “self-represented” under the electronic filing and service rules. Because Code of Civil Procedure section 1010.6 uses the term “unrepresented” and the rules use the term “self-represented,” the definition in the rules refers to self-represented parties or other persons as being those unrepresented by an attorney. This proposal was a suggestion from a member of the public.
- Amend rule 2.251(b) to require express consent for permissive electronic service. The current rules allows the act of electronic filing to serve as consent to electronic service. Effective January 1, 2019, Code of Civil Procedure section 1010.6 will no longer allow the act of electronic filing alone to serve as consent. (Code Civ. Proc, § 1010.6(a)(2)(A)(ii).) Under Code of Civil Procedure section 1010.6, parties may still consent through electronic means by “manifesting affirmative consent through electronic means with the court or the court’s electronic filing service provider, and concurrently providing the party’s electronic service address with that consent for the purpose of receiving electronic service.” The proposal amends the rules to remove the provision allowing the act of filing to serve as consent to electronic service and replace it with the language for manifesting affirmative consent by electronic means. Substantively, this is a technical amendment to ensure the rules comply with the statute. The proposal does not interpret the statute, however the committee seeks specific comments on whether there is a need for interpretation to provide more guidance to courts and electronic filing service providers.
- Amend rule 2.255 to add electronic filing managers within the scope of the rule. Code of Civil Procedure section 1010.6(g)(2) requires that “[a]ny system for the electronic filing and service of documents, including any information technology applications, Internet Web sites, and Web-based applications, used by an electronic service provider or any

other vendor or contractor that provides an electronic filing and service system to a trial court” be accessible by persons with disabilities and comply with certain access standards. Vendors and contractors must comply as soon as practicable, but no later than June 30, 2019. (Code Civ. Proc., § 1010.6(g)(3). Likewise, the statute requires the Judicial Council to adopt rules to implement the requirements as soon as practicable, but no later than June 30, 2019. (Code Civ. Proc., § 1010.6(g)(1). Code of Civil Procedure section 1010.6 includes specific requirements that courts and contractors must meet. Rule 2.255 already requires courts contracting with electronic filing service providers to comply with Code of Civil Procedure section 1010.6. However, because the rules do not account for contracts with electronic filing managers, the proposal amends rule 2.255 is amended to include them.

- Amend rule 2.255 to add subdivision (f) requiring require electronic filing service providers to allow filers to create an account without having to provide a credit card, debit card, or bank account information. The amendment is based on a suggestion from the State Bar Standing Committee on the Delivery of Legal Services. According to the standing committee, some electronic service providers require such payment information even if the filer is never charged. According to the standing committee, this “creates an insurmountable barrier to those without access to credit or banking services.” Subdivision (f) provides that it only applies to the creation of an account, but not to the provision of services unless the filer has a fee waiver.
- Amend rule 2.257 to create a procedure for electronically filed documents signed under penalty of perjury. Code of Civil Procedure section 1010.6(b)(2)(B)(ii) provides that when a document to be filed requires a signature made under penalty of perjury, the document is considered signed by the person if, in relevant part, “The person has signed the document using a computer or other technology pursuant to the procedure set forth in a rule of court adopted by the Judicial Council by January 1, 2019.” Accordingly, the proposal creates a procedure where the document is deemed signed when the “declarant has signed the document using an electronic signature, and declares under penalty of perjury that the information submitted is true and correct.” The language is modeled after the requirements in the Uniform Electronic Transactions Act for electronic signatures made under penalty of perjury. (Civ. Code, § 1633.11(b).) In addition, a definition of “electronic signature” is added to the rule modeled after the definitions used in UETA and the Code of Civil Procedure.

Alternatives Considered

The committee considered retaining the definitions of “electronic service,” “electronic transmission,” and “electronic notification” in rule 2.250(b) rather than referencing Code of Civil Procedure section 1010.6 for the definitions. The committee considered that referencing the Code of Civil Procedure will create an extra step in looking up the definitions. However, the committee opted for the proposed language to remove the risk of having differing definitions should the Legislature amend Code of Civil Procedure section 1010.6.

Implementation Requirements, Costs, and Operational Impacts

It is expected that the new express consent requirements will result in one-time costs to electronic filing service providers and courts to create a mechanism to capture affirmative consent by electronic means to electronic service. It is unknown whether or how these costs will impact fees electronic filing service providers charge filers for their services.

Request for Specific Comments

In addition to comments on the proposal as a whole, the advisory committee is interested in comments on the following:

- Does the proposal appropriately address the stated purpose?
- The technical amendments to rule 2.251(b) bring the rule into compliance with Code of Civil Procedure section 1010.6's express consent requirements. The rule does not interpret the express consent requirements. Is there a need for interpretation of the statute to provide guidance to the courts and electronic filing service providers? If so, what specific guidance is needed?

Attachments and Links

1. Proposed amendments to rules 2.250, 2.251, 2.255, and 2.257 of the California Rules of Court.
2. Code of Civil Procedure section 1010.6,
http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1010.6&lawCode=CCP.

1 Title 2. Trial Court Rules

2
3 Division 3. Filing and Service

4
5 Chapter 2. Filing and Service by Electronic Means

6
7 Rule 2.250. Construction and definitions

8
9 (a) * * *

10
11 (b) Definitions

12
13 As used in this chapter, unless the context otherwise requires:

14
15 (1) A “document” is a pleading, a paper, a declaration, an exhibit, or another
16 writing submitted by a party or other person, or by an agent of a party or
17 other person on the party’s or other person’s behalf. A document is also a
18 notice, order, judgment, or other issuance by the court. A document may be
19 in paper or electronic form.

20
21 (2) “Electronic service” has the same meaning as defined in Code of Civil
22 Procedure section 1010.6. ~~is service of a document on a party or other person~~
23 ~~by either electronic transmission or electronic notification. Electronic service~~
24 ~~may be performed directly by a party or other person, by an agent of a party~~
25 ~~or other person, including the party’s or other person’s attorney, through an~~
26 ~~electronic filing service provider, or by a court.~~

27
28 (3) “Electronic transmission” has the same meaning as defined in Code of Civil
29 Procedure section 1010.6. ~~means the transmission of a document by~~
30 ~~electronic means to the electronic service address at or through which a party~~
31 ~~or other person has authorized electronic service.~~

32
33 (4) “Electronic notification” has the same meaning as defined in Code of Civil
34 Procedure section 1010.6. ~~means the notification of a party or other person~~
35 ~~that a document is served by sending an electronic message to the electronic~~
36 ~~service address at or through which the party or other person has authorized~~
37 ~~electronic service, specifying the exact name of the document served and~~
38 ~~providing a hyperlink at which the served document can be viewed and~~
39 ~~downloaded.~~

40
41 (5) – (8) * * *

42

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

4
5 (10) “Self-represented” means a party or other person who is unrepresented in an
6 action by an attorney and does not include an attorney appearing in an action
7 who represents himself or herself.

8
9 **Rule 2.251. Electronic service**

10
11 **(a) * * ***

12
13 **(b) Electronic service by express consent of the parties**

14
15 (1) ~~Electronic service may be established by consent.~~ A party or other person
16 indicates that the party or other person agrees to accept electronic service by:

17
18 (A) Serving a notice on all parties and other persons that the party or other
19 person accepts electronic service and filing the notice with the court.
20 The notice must include the electronic service address at which the
21 party or other person agrees to accept service; or

22
23 (B) ~~Electronically filing any document with the court. The act of electronic~~
24 ~~filing is evidence that the party or other person agrees to accept service~~
25 ~~at the electronic service address the party or other person has furnished~~
26 ~~to the court under rule 2.256(a)(4). This subparagraph (B) does not~~
27 ~~apply to self-represented parties or other self-represented persons; they~~
28 ~~must affirmatively consent to electronic service under subparagraph~~
29 ~~(A). Manifesting affirmative consent through electronic means with the~~
30 court or the court’s electronic filing service provider, and concurrently
31 providing the party’s electronic service address with that consent for
32 the purpose of receiving electronic service.

33
34 (2) A party or other person that has consented to electronic service under (1) and
35 has used an electronic filing service provider to serve and file documents in a
36 case consents to service on that electronic filing service provider as the
37 designated agent for service for the party or other person in the case, until
38 such time as the party or other person designates a different agent for service.

39
40 **(c) - (k) * * ***

41

1 **Rule 2.255. Contracts with electronic filing service providers and electronic filing**
2 **managers**

3
4 **(a) Right to contract**

- 5
6 (1) A court may contract with one or more electronic filing service providers to
7 furnish and maintain an electronic filing system for the court.
8
9 (2) If the court contracts with an electronic filing service provider, it may require
10 electronic filers to transmit the documents to the provider.
11
12 (3) A court may contract with one or more electronic filing managers to act as an
13 intermediary between the court and electronic filing service providers.
14
15 ~~(3)~~(4) If the court contracts with an electronic service provider or the court has an
16 in-house system, the provider or system must accept filing from other
17 electronic filing service providers to the extent the provider or system is
18 compatible with them.
19

20 **(b) Provisions of contract**

- 21
22 (1) The court's contract with an electronic filing service provider may:
23
24 (A) Allow the provider to charge electronic filers a reasonable fee in
25 addition to the court's filing fee;
26
27 (B) Allow the provider to make other reasonable requirements for use of
28 the electronic filing system.
29
30 (2) The court's contract with an electronic filing service provider must comply
31 with requirements of Code of Civil Procedure section 1010.6.
32
33 (3) The court's contract with an electronic filing manager must comply with
34 requirements of Code of Civil Procedure section 1010.6.
35

36 **(c) Transmission of filing to court**

- 37
38 (1) An electronic filing service provider must promptly transmit any electronic
39 filing and any applicable filing fee to the court: directly or through the court's
40 electronic filing manager.
41
42 (2) An electronic filing manager must promptly transmit an electronic filing and
43 any applicable filing fee to the court.

1
2 **(d) Confirmation of receipt and filing of document**

- 3
4 (1) An electronic filing service provider must promptly send to an electronic filer
5 its confirmation of the receipt of any document that the filer has transmitted
6 to the provider for filing with the court.
7
8 (2) The electronic filing service provider must send its confirmation to the filer's
9 electronic service address and must indicate the date and time of receipt, in
10 accordance with rule 2.259(a).
11
12 (3) After reviewing the documents, the court must promptly transmit to the
13 electronic filing service provider and the electronic filer the court's
14 confirmation of filing or notice of rejection of filing, in accordance with rule
15 2.259.

16
17 **(e) Ownership of information**

18
19 All contracts between the court and electronic filing service providers or the court
20 and electronic filing managers must acknowledge that the court is the owner of the
21 contents of the filing system and has the exclusive right to control the system's use.
22

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

- 24
25 (1) An electronic filing service provider may not require a filer to provide a credit
26 card, debit card, or bank account information to create an account with the
27 electronic filing service provider.
28
29 (2) This provision applies only to the creation of an account and not to the use of
30 an electronic filing service provider's services. An electronic filing services
31 provider may require a filer to provide a credit card, debit card, or bank account
32 information before rendering services unless the services are within the scope
33 of a fee waiver granted by the court to the filer.
34

35 **Rule 2.257. Requirements for signatures on documents**

36
37 **(a) Electronic signature**

38
39 An electronic signature is an electronic sound, symbol, or process attached to or
40 logically associated with an electronic record and executed or adopted by a person
41 with the intent to sign a document or record created, generated, sent,
42 communicated, received, or stored by electronic means.
43

1 **(a)(b) Documents signed under penalty of perjury**

2
3 When a document to be filed electronically provides for a signature under penalty
4 of perjury of any person, the document is deemed to have been signed by that
5 person if filed electronically provided that either of the following conditions is
6 satisfied:

- 7
- 8 (1) The declarant has signed the document using an electronic signature a
9 computer or other technology, in accordance with procedures, standards, and
10 guidelines established by the Judicial Council and declares under penalty of
11 perjury under the laws of the state of California that the information
12 submitted is true and correct; or
- 13
- 14 (2) The declarant, before filing, has physically signed a printed form of the
15 document. By electronically filing the document, the electronic filer certifies
16 that the original, signed document is available for inspection and copying at
17 the request of the court or any other party. In the event this second method of
18 submitting documents electronically under penalty of perjury is used, the
19 following conditions apply:
- 20
- 21 (A) At any time after the electronic version of the document is filed, any
22 party may serve a demand for production of the original signed
23 document. The demand must be served on all other parties but need not
24 be filed with the court.
- 25
- 26 (B) Within five days of service of the demand under (A), the party or other
27 person on whom the demand is made must make the original signed
28 document available for inspection and copying by all other parties.
- 29
- 30 (C) At any time after the electronic version of the document is filed, the
31 court may order the filing party or other person to produce the original
32 signed document in court for inspection and copying by the court. The
33 order must specify the date, time, and place for the production and must
34 be served on all parties.
- 35
- 36 (D) Notwithstanding (A)–(C), local child support agencies may maintain
37 original, signed pleadings by way of an electronic copy in the statewide
38 automated child support system and must maintain them only for the
39 period of time stated in Government Code section 68152(a). If the local
40 child support agency maintains an electronic copy of the original,
41 signed pleading in the statewide automated child support system, it may
42 destroy the paper original.
- 43

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

2

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

4

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

6

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

8

9

Advisory Committee Comment

10

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

INVITATION TO COMMENT

[ItC prefix as assigned]-__

Title	Action Requested
Technology: Rules Modernization Project	Review and submit comments by June 8, 2018
Proposed Rules, Forms, Standards, or Statutes	Proposed Effective Date
Adopt Judicial Council Form EFS-006-CV.	January 1, 2019
Proposed by	Contact
Information Technology Advisory Committee	Andrea Jaramillo, 916-263-0991
Hon. Sheila F. Hanson, Chair	andrea.jaramillo@jud.ca.gov
Civil and Small Claims Advisory Committee	Anne Ronan, 415-865-8933
Hon. Ann I. Jones, Chair	anne.ronan@jud.ca.gov

Executive Summary and Origin

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

The Proposal

The proposed form is Judicial Council form EFS-006-CV, *Withdrawal of Consent to Electronic Service*. Under Code of Civil Procedure section 1010.6(a)(6), “A party or other person who has provided express consent to accept service electronically may withdraw consent at any time by completing and filing with the court the appropriate Judicial Council form. The Judicial Council shall create the form by January 1, 2019.” The proposed form is modeled after current form EFS-005-CV, *Consent to Electronic Service and Notice of Electronic Service Address*.

Alternatives Considered

Because the form is required by statute, no alternative was considered.

Implementation Requirements, Costs, and Operational Impacts

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

Attachments and Links.

1. Proposed Judicial Council form EFS-006-CV, *Withdrawal of Consent to Electronic Service*.
2. Code of Civil Procedure section 1010.6,
http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1010.6&lawCode=CCP.

ATTORNEY OR PARTY WITHOUT ATTORNEY: STATE BAR NO: NAME: FIRM NAME: STREET ADDRESS: CITY: STATE: ZIP CODE: TELEPHONE NO.: FAX NO. : E-MAIL ADDRESS: ATTORNEY FOR (name):	FOR COURT USE ONLY
SUPERIOR COURT OF CALIFORNIA, COUNTY OF STREET ADDRESS: MAILING ADDRESS: CITY AND ZIP CODE: BRANCH NAME:	CASE NUMBER:
Plaintiff/Petitioner: Defendant/Respondent:	JUDICIAL OFFICER:
WITHDRAWAL OF CONSENT TO ELECTRONIC SERVICE	DEPARTMENT:

1. The following party or the attorney for:

- a. plaintiff (name):
- b. defendant (name):
- c. petitioner (name):
- d. respondent (name):
- e. other (describe):

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

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

Street:
 City:
 State: Zip:

3. All notices and documents regarding the action shall be served on the person identified in item 1 at the address in item 2 as of (date):

Date: _____

TYPE OR PRINT NAME
(SIGNATURE OF PARTY OR ATTORNEY)

CASE NAME:	CASE NUMBER:
------------	--------------

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

PROOF OF ELECTRONIC SERVICE
WITHDRAWAL OF CONSENT TO ELECTRONIC SERVICE

1. I am at least 18 years old.

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

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

a. Name of person served:

b. Electronic service address of person served:

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

c. On (*date*):

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

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

Date:

(TYPE OR PRINT NAME OF DECLARANT)

(SIGNATURE OF DECLARANT)

INVITATION TO COMMENT

[ItC prefix as assigned]-__

Title	Action Requested
Technology: Remote Access to Electronic Records	Review and submit comments by June 8, 2018
Proposed Rules, Forms, Standards, or Statutes	Proposed Effective Date
Amend Cal. Rules of Court, rules 2.500—2.503; adopt rules 2.515—2.528 and rules 2.540—2.545.	January 1, 2019
Proposed by	Contact
Information Technology Advisory Committee	Andrea L. Jaramillo, (916) 263-0991
Hon. Sheila F. Hanson, Chair	andrea.jaramillo@jud.ca.gov

Executive Summary and Origin

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 and provide clear authority to the courts.

The project to develop the new rules originated with the *California Judicial Branch Tactical Plan for Technology (2017-2018)*. Under the tactical plan, a major task under the “Technology Initiatives to Promote Rule and Legislative Changes” is to develop rules “for online access to court records for parties and justice partners[.]” (Judicial Council of Cal., *California Judicial Branch Tactical Plan for Technology (2017-2018)* (2017), p. 47.)

Background

Existing rules govern public access to electronic trial court records (Cal. Rules of Court, rules 2.500—2.507), but do not govern access to such records by parties, their attorneys, or justice partners. (See Cal. Rules of Court, rule 2.501(b).) Because courts are moving swiftly forward with making remote access to records available to these persons and entities, it is important to provide authority and guidance for the courts and others on these expanded forms of remote access.

Under the leadership of the Information Technology Committee (ITAC), nine advisory committees¹ formed the Joint Ad Hoc Subcommittee on Remote Access to develop remote access rules applicable to parties, their attorneys, and justice partners. The formation of the Joint Ad Hoc Subcommittee for this purpose was approved by the advisory bodies' internal oversight committees.

The Proposal

The existing rules governing electronic access to trial court records are found in of chapter 2 of division 4 of title 2 of the California Rules of Court (hereafter, chapter 2). Chapter 2's rules currently apply "only to access to court records by the public" and limit what is remotely accessible by the public to registers of action, calendars, indexes, and court records in specific case types. (Cal. Rules of Court, rules 2.501(b), 2.503(b).) The rules in chapter 2 "do not limit access to court records by a party to an action or proceeding, by the attorney of a party, or by other persons or entities that are entitled to access by statute or rule." (Rule 2.501(b).)

Because chapter 2 only limits *public* remote access, there is a gap in the rules with respect to persons and entities that are not the public at large such as parties, parties' attorneys, and justice partners. Courts have had to fill this gap on a piecemeal, ad hoc basis. The purpose of the proposal is to create a new set of rules applicable statewide governing remote access to electronic records to provide more structure, guidance, and authority for the courts. The proposal does not create a right to remote access and it does not provide for a higher level of access to court records using remote access than one would get by viewing court records at the courthouse.

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

- **Article 1: General Provisions.** This article builds on existing rules, covers broad concepts on access to electronic records, and expands on the definitions of terms used in chapter 2.
- **Article 2: Public Access.** This article consists of the existing public access rules, with minor amendments.
- **Article 3: Remote Electronic Access by a Party, Party's Attorney, Court-Appointed Person, or Authorized Persons Working in a Legal Organization or Qualified Legal Services Project.** The content of this article is new and covers remote electronic access by those listed in the article's title.

¹ ITAC, Appellate Advisory Committee, Family and Juvenile Law Advisory Committee, Probate and Mental Health Advisory Committee, Advisory Committee on Providing Access and Fairness, Traffic Advisory Committee, Civil and Small Claims Advisory Committee, Criminal Law Advisory Committee, and Tribal Court-State Court Forum.

- **Article 4: Remote Electronic Access by Government Entities.** The content of this article is new and covers remote electronic access by government entities.

Article 1: General Provisions

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

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

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

The proposal amends subdivision (b) by striking out the existing language and replacing it with a new provision. The existing language is stricken out because the rules of the chapter in the proposal expand the scope beyond public access and so the limitations in the existing language are no longer applicable. Because the new rules expand the scope of remote access by allowing a greater level of remote access by certain persons and entities, the new provision requires courts to provide information to the public on who may access their court records under the rules of the chapter. Courts may provide the information by linking to information that will be publicly posted on courts.ca.gov and may also supplement with information on their own sites in plain language.

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

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

Article 2: Public Access

Article 2 largely retains the existing public access rules found in rules 2.503—2.507. Rule 2.503 is the only one of these rules with substantive amendments and those amendments are minor. The amendments clarify that the rules in article 2 only apply to access to electronic records by the public.

The amendments also make a technical change to the list of electronic records to which a court must provide for electronic access by the public. Under rule 2.503(b), all records in civil cases must be available remotely, if feasible, except for those listed in rule 2.503(c)(1)—(9). Rule 2.503(c) lists all the case types where electronic access must be provided at the courthouse, but must not be provided remotely. However, under rule 2.503(c) there are ten case types, not nine. The omission in rule 2.503(b) of the tenth case type was accidental. Rule 2.503(c) was amended effective January 1, 2012 with an addition of a tenth case type, but there was no corresponding amendment to the reference to the list in rule 2.503(b). The proposal corrects the incongruity between subdivisions (b) and (c) of rule 2.503.

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

Article 3 contains new rules to cover remote electronic access by a party, party’s attorney, court-appointed person, or authorized persons working in a legal organization or qualified legal services project. Each of these types of remote accessors are discussed below. The rules make clear that article 3 is not intended to limit remote electronic access available under article 2 (the public access rules). Accordingly, if someone could have remote electronic access to a court record under article 2, that person may do so without meeting the requirements of article 3. The rules under article 3, like the public access rules, require courts to provide remote electronic access if it is feasible to do so. Finally, the rules in article 3 include requirements for identity verification, security of confidential information, and additional conditions of access.

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

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

Rule 2.516. Remote access to extent feasible. The proposed rule requires courts to allow remote access to electronic records to the types of users identified in rule 2.515. This is similar to the

public access requirement existing in rule 2.503. The advisory committee comment recognizes financial means of technical capabilities may impact the feasibility of providing remote access.

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

Rule 2.518. Remote access by a party’s designee. The proposed rule allows a party who is a natural person to designate other persons to access the party’s electronic records provided that the party is at least 18 years of age. The rule allows the party to set limits on the designee’s access such as to specific cases or for a specific period of time. In addition, the designee may only have the same access to a party’s electronic records that a member of the public would be entitled to if he or she were to inspect the party’s court records at the courthouse. For example, if a court record is sealed and the designee would not be entitled to view the court record at the courthouse, the designee cannot remotely access the electronic record. The rule sets forth basic terms of access, though there may be additional terms in a user agreement set by the court. The rule does not prescribe a particular method for establishing a designation as this may depend on the preferences and technical capabilities of individual courts.

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

Attorneys who are attorneys of record should be known to the court for remote access purposes since they are of record. The rule also accounts for providing remote access to attorneys who are not the attorneys of record in an underlying proceeding who may nonetheless be assisting a party. For example, an attorney may be assisting a party with limited aspects of their case, like document preparation, without becoming the attorney of record. Rule 2.518(c) requires an attorney who is not of record to obtain the party’s consent to remotely access the party’s court records and represent to the court in the remote access system that the attorney has obtained the party’s consent. This provides a mechanism for an attorney not of record to be known to the court and provides the court with assurance that the party has agreed to allow the attorney to remotely access the party’s electronic records. The proposed rule also sets forth basic terms of access.

Rule 2.520. Remote access by persons working in the same legal organization as a party’s attorney. Because attorneys often work with other attorneys and legal staff, proposed rule 2.519

allows remote access by persons “working in” the same “legal organization” as a party’s attorney. Both “legal organization” and “working in” are broad in scope. Under the definitions in rule 2.502, “legal organization” means “a licensed attorney or group of attorneys, nonprofit legal aid organization, government legal office, in-house legal office of a non-governmental organization, or legal program organized to provide for indigent criminal, civil, or juvenile law representation.” Those “working in” the same legal organization as a party’s attorney may include partners, associates, employees, volunteers, and contractors. The goal with the definition of “legal organization” and the scope of “working in” is intended to capture a full range of ways that attorneys may be working together and with others to provide representation to a party.

Under rule 2.519, a party’s attorney can designate other persons working in the same legal organization to have remote access and the attorney must certify that those persons are working in the same legal organization and assisting the attorney with the party’s case. The rule does not require certification to take any specific form. The proposed rule also sets forth basic terms of access.

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

Rule 2.522. Remote access by persons working in a qualified legal services project providing brief legal services. The proposed rule allows remote access to electronic records by persons “working in” a “qualified legal services project” providing “brief legal services.” The rule contemplates legal aid programs offering limited, short-term services to individuals with their court matters.

“Brief legal services” for purposes of chapter 2 is defined in rule 2.502 and means “legal assistance provided without, or prior to, becoming a party’s attorney. It includes advice, consultation, research, investigating case facts, drafting documents, and making limited third party contacts on behalf of a client.”

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

- (1) A nonprofit project incorporated and operated exclusively in California that provides as its primary purpose and function legal services without charge to indigent persons and that has quality control procedures approved by the State Bar of California.

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

Where an attorney from a qualified legal services project does become a party's attorney and offers services beyond the scope contemplated under this rule, the remote access rules for a party's attorney would also provide a mechanism for access as could the party's designee rule. The proposed rule also sets forth basic terms of access.

Rule 2.523. Identity verification, identity management, and user access. The proposed rule requires a court to verify of a person eligible to have remote access to electronic records under article 3. Subdivision (b) describes the responsibilities of the court to verify identities and provide unique credentials to users. The rule does not prescribe any particular mechanism for identity verification or credentials as the best solutions may differ from court-to-court. Subdivision (c) describes responsibilities of users to provide necessary information for identity verification, consent to conditions of access, and only access the records the user is authorized to access. Subdivision (d) describes responsibilities of legal organizations and qualified legal services projects to verify the identity of users it designates and notify the court when a user is no longer working in the legal organization or qualified legal services project. Subdivision (e) makes it clear that courts may enter into contracts or participate in statewide master agreements for identity verification, identity management, or access management systems.

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

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

Rule 2.526. Audit trails. The purpose of the proposed rule is to ensure courts are able to see who remotely accessed electronic records, under whose authority the user gained access, what electronic records were accessed, and under whose authority the user gained access. The audit trail is a tool to assist the courts in identifying and investigating any potential issues or misuse of remote access. The rule also requires the court to provide limited audit trails to authorized users remotely accessing remote records under article 3. The limited audit trail would only show who remotely access electronic records in a particular case, but would not show which specific electronic records were accessed. The reason for this more limited view at the case level rather than individual electronic record level is to protect confidential information.

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

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

Article 4: Remote Electronic Access by Government Entities

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

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

The proposed rule does not preclude government entities from gaining access to court records through articles 2 and 3. The proposed rule does not grant higher levels of access to court records

than currently exists. Rather, like with the rules under article 3, it only provides for remote access to records that the government entity would be able to obtain if its agents appeared at the courthouse to inspect the records in person.

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

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

Rule 2.543. Audit trails. The proposed rule mirrors rule 2.526 requiring the court to be able to generate audit trails and provide limited audit trails to authorized users.

Rule 2.544. Additional conditions of access. The proposed rule mirrors rule 2.527 requiring courts to impose reasonable conditions of access.

Rule 2.545. Termination of remote access. The proposed rule makes clear that remote access to electronic records is a privilege and not a right and that courts may terminate any grant of permission for remote access.

Implementation Requirements, Costs, and Operational Impacts

The rules require the courts to provide remote access under the new rules if it is feasible to do so and the rules recognize that financial and technological limitations may impact the feasibility of providing remote access. If feasible, implementation would require courts to create user agreements and have systems capable of complying with the rules. Costs and specific implementation requirements would be variable across the courts depending on current capabilities and approach to providing services.

Request for Specific Comments

In addition to comments on the proposal as a whole, the advisory committee is interested in comments on the following:

- Does the proposal appropriately address the stated purpose?
- Proposed rule 2.518 would allow a person who is a party and who is 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?
- The reference to "concurrent jurisdiction" in proposed rule 2.540(b)(1)(xi) is intended to capture cases in which a tribal entity would have a right to access the court records at the court depending on the nature of the case and type of tribal involvement. Is "concurrent jurisdiction" the best way to describe such cases or would a different phrasing be more accurate?
- Is the standard for "good cause" in proposed rule 2.540(b)(1)(xii) clear?
- The proposed rules have some internal redundancies. This was intentional in development of the rules 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 access" in article 4 repeat 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 repeat in articles 4 and 5. Does the organization of the rules, including the redundant language, provide clear guidance? Would another organizational scheme be clearer?

The advisory committee also seeks comments from *courts* on the following cost and implementation matters:

- Would the proposal provide cost savings? If so please quantify.
- 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.
- What implementation guidance, if any, would courts find helpful?

Attachments and Links

1. Proposed rules 2.500, 2.501, 2.502, 2.503, 2.515, 2.516, 2.517, 2.518, 2.519, 2.520, 2.521, 2.522, 2.523, 2.524, 2.525, 2.526, 2.527, 2.528, 2.540, 2.541, 2.542, 2.543, 2.544, and 2.545 of the California Rules of Court.

1 **Title 2. Trial Court Rules**

2
3 **Division 1. General Provisions**

4
5 **Chapter 2. ~~Public~~-Access to Electronic Trial Court Records**

6
7 **Article 1. General Provisions**

8
9 **Rule 2.500. Statement of purpose**

10
11 **(a) Intent**

12
13 The rules in this chapter are intended to provide the public, parties, parties'
14 attorneys, legal organizations, court-appointed persons, and government entities
15 with reasonable access to trial court records that are maintained in electronic form,
16 while protecting privacy interests.

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

26
27 **(c) No creation of rights**

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

34
35 **Advisory Committee Comment**

36
37 The rules in this chapter acknowledge the benefits that electronic ~~court~~ records provide but
38 attempt to limit the potential for unjustified intrusions into the privacy of individuals involved in
39 litigation that can occur as a result of remote access to electronic ~~court~~ records. The proposed
40 rules take into account the limited resources currently available in the trial courts. It is
41 contemplated that the rules may be modified to provide greater electronic access as ~~the courts~~²

1 technical capabilities improve and ~~with the knowledge is~~ gained from the experience of ~~the courts~~
2 ~~in~~ providing electronic access under these rules.

3
4
5 **Rule 2.501. Application, and scope, and information to the public**

6
7 **(a) Application and scope**

8
9 The rules in this chapter apply only to trial court records as defined in Rule 2.502
10 (4). They do not apply to statutorily mandated reporting between or within
11 government entities, the California Courts Protective Order Registry, or any other
12 documents or materials that are not court records.

13
14 **~~Access by parties and attorneys~~ Information to the public**

15
16 ~~The rules in this chapter apply only to access to court records by the public. They~~
17 ~~do not limit access to court records by a party to an action or proceeding, by the~~
18 ~~attorney of a party, or by other persons or entities that are entitled to access by~~
19 ~~statute or rule.~~

20
21 The website for each trial court must include a link to information that will inform
22 the public of who may access their electronic records under the rules in this chapter
23 and under what conditions they may do so. This information will be posted publicly
24 on www.courts.ca.gov. Each trial court may post additional information, in plain
25 language, as necessary to inform the public about the level of access that the
26 particular trial court is providing.

27
28 **Advisory Committee Comment**

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

1
2 **Rule 2.502. Definitions**
3

4 As used in this chapter, the following definitions apply:
5

6 (1) “Authorized person” means a person authorized by a legal organization, qualified
7 legal services project, or government entity to access electronic records.
8

9 (2) “Brief legal services” means legal assistance provided without, or before, becoming
10 a party’s attorney. It includes advice, consultation, research, investigating case
11 facts, drafting documents, and making limited third party contacts on behalf of a
12 client.
13

14 ~~(3)~~(3) “Court record” is any document, paper, or exhibit filed by the parties to in an action
15 or proceeding; any order or judgment of the court; and any item listed in
16 Government Code section 68151(a), excluding any reporter’s transcript for which
17 the reporter is entitled to receive a fee for any copy, that is maintained by the court
18 in the ordinary course of the judicial process. The term does not include the
19 personal notes or preliminary memoranda of judges or other judicial branch
20 personnel, materials in the California Courts Protective Order Registry, statutorily
21 mandated reporting between or within government entities, judicial administrative
22 records, court case information, or compilations of data drawn from court records
23 where the compilations are not themselves contained in a court record.
24

25 (4) “Court case information” consists of information created and maintained by a court
26 about a case or cases that is not part of the court records that are filed with the court.
27 This includes information in the case management system and case histories.
28

29 ~~(4)~~(5) “Electronic access” means computer access by electronic means to court records
30 available to the public through both public terminals at the courthouse and
31 remotely, unless otherwise specified in the rules in this chapter.
32

33 ~~(2)~~(6) “Electronic record” is a computerized court record that requires the use of an
34 electronic device to access, regardless of the manner in which it has been
35 computerized. The term includes both a document record that has been filed
36 electronically and an electronic copy or version of a record that was filed in paper
37 form. The term does not include a court record that is maintained only on paper,
38 microfiche, or any other medium that can be read without the use of an electronic
39 device.
40

41 (7) “Government entity” means a legal entity organized to carry on some function of
42 the State of California or a political subdivision of the State of California. A

1 government entity is also a federally recognized Indian tribe or a reservation,
2 department, subdivision, or court of a federally recognized Indian tribe.

3
4 (8) “Legal organization” means a licensed attorney or group of attorneys, nonprofit
5 legal aid organization, government legal office, in-house legal office of a non-
6 governmental organization, or legal program organized to provide for indigent
7 criminal, civil, or juvenile law representation.

8
9 (9) “Party” means a plaintiff, defendant, cross-complainant, cross-defendant,
10 petitioner, respondent, intervenor, objector, or anyone expressly defined by statute
11 as a party in a court case.

12
13 (10) “Person” means a natural human being.

14
15 ~~(3)~~(11) “The public” means a person, a group, or an entity, including print or electronic
16 media, or the representative of an individual, a group, or an entity regardless of any legal
17 or other interest in a particular court record.

18
19 (12) “Qualified legal services project” has the same meaning under the rules of this
20 chapter as in 6213(a) of the Business and Professions Code.

21
22 (13) “Remote access” means electronic access from a location other than a public
23 terminal at the courthouse.

24
25 (14) “User” means an individual person, a group, or an entity that accesses electronic
26 records.

27 28 Article 2. Public Access

29 30 **Rule 2.503. ~~Public access~~ Application and scope**

31 32 **(a) General right of access by the public**

33
34 (1) All electronic records must be made reasonably available to the public in
35 some form, whether in electronic or in paper form, except those that are sealed by
36 court order or made confidential by law.

37
38 (2) The rules in this article apply only to access to electronic records by the
39 public.

40 41 **(b) Electronic access required to extent feasible**

42

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

4
5 (1) * * *

6
7 (2) All records in civil cases, except those listed in (c)(1)–~~(9)~~(10).

8
9 **(c) Courthouse electronic access only**

10
11 A court that maintains the following records in electronic form must provide
12 electronic access to them at the courthouse, to the extent it is feasible to do so, but
13 may provide public remote ~~electronic~~ access only to the records ~~governed by~~
14 specified in subsection (b):

15
16 ~~(1)–(10)~~ * * *

17
18 **(d) * * ***

19
20 **(e) Remote ~~electronic~~ access allowed in extraordinary criminal cases**

21
22 Notwithstanding (c)(5), the presiding judge of the court, or a judge assigned by the
23 presiding judge, may exercise discretion, subject to (e)(1), to permit remote
24 ~~electronic~~ access by the public to all or a portion of the public court records in an
25 individual criminal case if (1) the number of requests for access to documents in
26 the case is extraordinarily high and (2) responding to those requests would
27 significantly burden the operations of the court. An individualized determination
28 must be made in each case in which such remote ~~electronic~~ access is provided.

29
30 (1) In exercising discretion under (e), the judge should consider the relevant
31 factors, such as:

32
33 (A) * * *

34
35 (B) The benefits to and burdens on the parties in allowing remote ~~electronic~~
36 access, including possible impacts on jury selection; and

37
38 (C) * * *

39
40 (2) The court should, to the extent feasible, redact the following information
41 from records to which it allows remote access under (e): driver license
42 numbers; dates of birth; social security numbers; Criminal Identification and
43 Information and National Crime Information numbers; addresses and phone

1 numbers of parties, victims, witnesses, and court personnel; medical or
2 psychiatric information; financial information; account numbers; and other
3 personal identifying information. The court may order any party who files a
4 document containing such information to provide the court with both an
5 original unredacted version of the document for filing in the court file and a
6 redacted version of the document for remote ~~electronic~~ access. No juror
7 names or other juror identifying information may be provided by remote
8 ~~electronic~~ access. This subdivision does not apply to any document in the
9 original court file; it applies only to documents that are available by remote
10 ~~electronic~~ access.

11
12 (3) Five days' notice must be provided to the parties and the public before the
13 court makes a determination to provide remote ~~electronic~~ access under this
14 rule. Notice to the public may be accomplished by posting notice on the
15 court's Web site. Any person may file comments with the court for
16 consideration, but no hearing is required.

17
18 (4) The court's order permitting remote ~~electronic~~ access must specify which
19 court records will be available by remote ~~electronic~~ access and what
20 categories of information are to be redacted. The court is not required to
21 make findings of fact. The court's order must be posted on the court's Web
22 site and a copy sent to the Judicial Council.

23
24 **(f)-(i) * * ***

25
26 **Advisory Committee Comment**

27
28 The rule allows a level of access by the public to all electronic records that is at least equivalent
29 to the access that is available for paper records and, for some types of records, is much greater. At
30 the same time, it seeks to protect legitimate privacy concerns.

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

1 determinations in a specific case, certain records in criminal cases may be made available over
2 the Internet.

3
4 **Subdivisions (f) and (g).** These subdivisions limit electronic access to records (other than the
5 register, calendars, or indexes) to a case-by-case basis and prohibit bulk distribution of those
6 records. These limitations are based on the qualitative difference between obtaining information
7 from a specific case file and obtaining bulk information that may be manipulated to compile
8 personal information culled from any document, paper, or exhibit filed in a lawsuit. This type of
9 aggregate information may be exploited for commercial or other purposes unrelated to the
10 operations of the courts, at the expense of privacy rights of individuals.

11
12 Courts must send a copy of the order permitting remote ~~electronic~~ access in extraordinary
13 criminal cases to: Criminal Justice Services, Judicial Council of California, 455 Golden Gate
14 Avenue, San Francisco, CA 94102-3688.

15
16 **Rule 2.504-2.507 * * ***

17
18 **Article 3. Remote Access by a Party, Party's Attorney, Court-Appointed Person, or**
19 **Authorized Person Working in a Legal Organization or Qualified Legal**
20 **Services Project**

21
22 **Rule 2.515. Application and scope**

23
24 **(a) No limitation on access to electronic records available through article 2**

25
26 The rules in this article do not limit remote access to electronic records available
27 under article 2.

28
29 **(b) Who may access**

30
31 The rules in this article apply to remote access to electronic records by:

32
33 (1) A person who is a party;

34
35 (2) A party's attorney;

36
37 (3) An authorized person working in the same legal organization as a party's
38 attorney;

39
40 (4) An authorized person working in a qualified legal services project providing
41 brief legal services;

42
43 (5) A court-appointed person.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39

Advisory Committee Comment

Article 2 allows remote access in most civil cases and the rules in article 3 are not intended to limit that access. Rather, the article 3 rules allow broader remote access by parties, parties’ attorneys, authorized persons working in legal organizations, authorized persons working in a qualified legal services project providing brief services, and court-appointed persons to those electronic records where remote access by the public is not allowed.

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

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

Rule 2.516. Remote access to extent feasible

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

Advisory Committee Comment

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

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

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

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

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

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

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

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

21
22 **Advisory Committee Comment**

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

28
29 **Rule 2.518. Remote access by a party's designee**

30
31 **(a) Remote access generally permitted**

32
33 A person, who is at least 18 years of age, may designate other persons to have
34 remote access to electronic records in actions or proceedings in which that
35 person is a party.

36
37 **(b) Level of remote access**

38
39 (1) A party's designee may have the same access to a party's electronic records
40 that a member of the public would be entitled to if he or she were to inspect
41 the party's court records at the courthouse.

42

1 probate proceeding, the court may grant remote access to that attorney before
2 an order of appointment is issued by the court.

3
4 **(b) Level of remote access**

5
6 A party's attorney may be provided remote access to the same electronic records in
7 the party's actions or proceedings that the party's attorney would be legally entitled
8 to view at the courthouse.

9
10 **(c) Terms of remote access for attorneys who are not the attorney of record in the**
11 **party's actions or proceedings in the trial court**

12
13 An attorney who represents a party, but who is not the party's attorney of record,
14 may remotely access the party's electronic records, provided that the attorney:

15
16 (1) Obtains the party's consent to remotely access the party's electronic records.

17
18 (2) Represents to the court in the remote access system that the attorney has
19 obtained the party's consent to remotely access the party's electronic records.

20
21 **(d) Terms of remote access for all attorneys accessing electronic records**

22
23 (1) A party's attorney may remotely accesses the electronic records only for the
24 purposes of assisting the party with the party's court matter.

25
26 (2) A party's attorney may not distribute for sale any electronic records obtained
27 remotely under the rules in this article. Such sale is strictly prohibited.

28
29 (3) A party's attorney must comply with any other terms of remote access required
30 by the court.

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

34
35 **Advisory Committee Comment**

36
37 **Subdivision (c).** An attorney of record will be known to the court for purposes of remote access.
38 However, there may be circumstances when a person engages an attorney for assistance, but that
39 attorney is not the attorney of record in an action or proceeding in which the person is a party.
40 Examples include, but are not limited to, when a party engages an attorney to (1) prepare legal
41 documents, but not appear in the party's action (e.g., provide limited scope representation); (2)
42 assist the party with dismissal/expungement or sealing of a criminal record where the attorney did
43 not represent the party in the criminal proceeding; or (3) represent the party in an appellate matter

1 when the attorney did not represent the party in the trial court. Subdivision (c) provides a
2 mechanism for an attorney not of record to be known to the court for purposes of remote access.

3
4 **Rule 2.520. Remote access by persons working in the same legal organization as a**
5 **party's attorney**

6
7 **(a) Application and scope**

8
9 (1) This rule applies when a party's attorney is assisted by others working in the
10 same legal organization.

11
12 (2) "Working in the same legal organization" under this rule includes partners,
13 associates, employees, volunteers, and contractors.

14
15 (3) This rule does not apply when a person working in the same legal organization
16 as a party's attorney gains remote access to records as a party's designee under
17 rule 2.518.

18
19 **(b) Designation and certification**

20
21 (1) A party's attorney may designate that other persons working in the same
22 legal organization as the party's attorney have remote access.

23
24 (2) A party's attorney must certify that the other persons authorized for access
25 are working in the same legal organization as the party's attorney and are
26 assisting the party's attorney in the action or proceeding.

27
28 **(c) Level of remote access**

29
30 (1) Persons designated by a party's attorney under subdivision (b) must be
31 provided access to the same electronic records as the party.

32
33 (2) Notwithstanding subdivision (b), when a court designates a legal organization
34 to represent parties in criminal, juvenile, family, or probate proceedings, the
35 court may grant remote access to a person working in the organization who
36 assigns cases to attorneys working in that legal organization.

37
38 **(d) Terms of remote access**

39
40 (1) Persons working in a legal organization may remotely access electronic records
41 only for purposes of assigning or assisting a party's attorney.

42

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

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

6
7 (4) Persons working in a legal organization must comply with any other terms of
8 remote access required by the court.

9
10 (5) Failure to comply with these rules may result in the imposition of sanctions
11 including termination of access.

12
13 **Rule 2.521. Remote access by a court-appointed person**

14
15 **(a) Remote access generally permitted**

16
17 (1) A court may grant a court-appointed person remote access to electronic records
18 in any action or proceeding in which the person has been appointed by the
19 court.

20
21 (2) Court-appointed persons include an attorney appointed to represent a minor
22 child under Family Code section 3150; a Court Appointed Special Advocate
23 volunteer in a juvenile proceeding; an attorney appointed under Probate Code
24 section 1470, 1471, or 1474; an investigator appointed under Probate Code
25 section 1454; a probate referee designated under Probate Code section 8920; a
26 fiduciary, as defined in Probate Code section 39; an attorney appointed under
27 Welfare and Institutions Code section 5365; or a guardian ad litem appointed
28 under Code of Civil Procedure section 372 or Probate Code section 1003.

29
30 **(b) Level of remote access**

31
32 A court-appointed person may be provided with the same level of remote access to
33 electronic records as the court-appointed person would be legally entitled if he or
34 she were to appear at the courthouse to inspect the court records.

35
36 **(c) Terms of remote access**

37
38 (1) A court-appointed person may remotely access electronic records only for
39 purposes of fulfilling the responsibilities for which he or she was appointed.

40
41 (2) Any distribution for sale of electronic records obtained remotely under the rules
42 in this article is strictly prohibited.

43

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

3
4 (4) A court-appointed person must comply with any other terms of remote access
5 required by the court.

6
7 (5) Failure to comply with these rules may result in the imposition of sanctions
8 including termination of access.

9
10 **Rule 2.522. Remote access by persons working in a qualified legal services project**
11 **providing brief legal services**

12
13 **(a) Application and scope**

14
15 (1) This rule applies to qualified legal services projects as defined in section
16 6213(a) of the Business and Professions Code.

17
18 (2) “Working in a qualified legal services project” under this rule means
19 attorneys, employees, and volunteers.

20
21 (3) This rule does not apply to a person working in or otherwise associated with
22 a qualified legal services project who gains remote access to court records as
23 a party’s designee under rule 2.518.

24
25 **(b) Designation and certification**

26
27 (1) A qualified legal services project may designate persons working in the
28 qualified legal services project who provide brief legal services, as defined in
29 article 1, to have remote access.

30
31 (2) The qualified legal services project must certify that the authorized persons
32 work in their organization.

33
34 **(c) Level of remote access**

35
36 Authorized persons may be provided remote access to the same electronic
37 records to which the authorized person would be legally entitled to inspect at
38 the courthouse.

39
40 **(d) Terms of remote access**

41
42 (1) Qualified legal services projects must obtain the party’s consent to remotely
43 access the party’s electronic records.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43

- (2) Authorized persons must represent to the court in the remote access system that the qualified legal services project has obtained the party’s consent to remotely access the party’s electronic records.
- (3) Qualified legal services projects providing services under this rule may remotely access electronic records only to provide brief legal services.
- (4) Any distribution for sale of electronic records obtained under the rules in this article is strictly prohibited.
- (5) All laws governing confidentiality and disclosure of court records apply to electronic records obtained under this article.
- (6) Qualified legal services projects must comply with any other terms of remote access required by the court.
- (7) Failure to comply with these rules may result in the imposition of sanctions including termination of access.

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

(a) Identity verification required

Before allowing a person who is eligible under the rules in article 3 to have remote access to electronic records, a court must verify the identity of the person seeking access.

(b) Responsibilities of the court

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

(c) Responsibilities of persons accessing records

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

- 1 (1) Provides the court with all information it directs in order to identify the person to
2 be a user;
3
4 (2) Consents to all conditions for remote access required by article 3 and the court;
5 and
6
7 (3) Is authorized by the court to have remote access to electronic records.
8

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

- 10
11 (1) If a person is accessing electronic records on behalf of a legal organization or
12 qualified legal services project, the organization or project must approve granting
13 access to that person, verify the person's identity, and provide the court with all
14 the information it directs in order to authorize that person to have access to
15 electronic records.
16
17 (2) If a person accessing electronic records on behalf of a legal organization or
18 qualified legal services project leaves his or her position or for any other reason is
19 no longer entitled to access, the organization or project must immediately notify
20 the court so that it can terminate the person's access.
21

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

24
25 A court may enter into a contract with a vendor to provide identity verification,
26 identity management, or user access services. Alternatively, if a statewide identity
27 verification, identity management, or access management system, or a statewide
28 master agreement for such systems is available, courts may use those for identity
29 verification, identity management, and user access services.
30

31 **Rule 2.524. Security of confidential information**

32
33 **(a) Secure access and encryption required**

34
35 If any information in an electronic record that is confidential by law or sealed by
36 court order may lawfully be provided remotely to a person or organization
37 described in rule 2.515, any remote access to the confidential information must be
38 provided through a secure platform and any electronic transmission of the
39 information must be encrypted.
40

41 **(b) Vendor contracts and statewide master agreements**
42

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

4
5 **Advisory Committee Comment**

6
7 This rule describes security and encryption requirements while levels of access are provided for
8 in rules 2.517–2.522.

9
10 **Rule 2.525. Searches and access to electronic records in search results**

11
12 **(a) Searches**

13
14 A user authorized under this article to remotely access a party’s electronic records
15 may search for the records by case number or case caption.

16
17 **(b) Access to electronic records in search results**

18
19 A court providing remote access to electronic records under this article must ensure
20 that authorized users are only able to access the electronic records at the levels
21 provided in this article.

22
23 **(c) Unauthorized access**

24
25 If a user gains access to an electronic record that the user is not authorized to access
26 under this article, the user must:

27
28 (1) Report the unauthorized access to the court as directed by the court for that
29 purpose;

30
31 (2) Destroy all copies, in any form, of the record; and

32
33 (3) Delete from the user’s browser history all information that identifies the record.

34
35 **Rule 2.526. Audit trails**

36
37 **(a) Ability to generate audit trails required**

38
39 The court must have the ability to generate an audit trail that identifies each
40 remotely accessed record, when an electronic record was remotely accessed, who
41 remotely accessed the electronic record, and under whose authority the user gained
42 access to the electronic record.

43

1 **(b) Limited audit trails available to authorized users**

2
3 (1) A court providing remote access to electronic records under this article must
4 make limited audit trails available to authorized users under this article

5
6 (2) A limited audit trail must show the user who remotely accessed electronic
7 records in a particular case, but must not show which specific electronic records
8 were accessed.

9
10 **Rule 2.527. Additional conditions of access**

11
12 To the extent consistent with these rules and other applicable law, a court must
13 impose reasonable conditions on remote access to preserve the integrity of its
14 records, prevent the unauthorized use of information, and limit possible legal
15 liability. The court may choose to require each user to submit a signed, written
16 agreement enumerating those conditions before it permits that user to remotely
17 access electronic records. The agreements may define the terms of access, provide
18 for compliance audits, specify the scope of liability, and provide for the imposition
19 of sanctions for misuse up to and including termination of remote access.

20
21 **Rule 2.528. Termination of remote access**

22
23 **(a) Remote access a privilege**

24
25 Remote access to electronic records 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 eligible under the rules in article 3 to remotely access electronic records at
31 any time for any reason.

32
33

1 Article 4. Remote Access by Government Entities

2
3 Rule 2.540. Application and scope

4
5 (a) Applicability to government entities

6
7 The rules in this article provide for remote access to electronic records by
8 government entities described in subsection (b) below. The access allowed under
9 these rules is in addition to any access these entities or authorized persons working
10 for such entities may have under the rules in articles 2–3.

11
12 (b) Level of remote access

13
14 (1) A court may provide authorized persons from government entities with remote
15 access to electronic records as follows:

16
17 (i) Office of the Attorney General: criminal electronic records and juvenile
18 justice electronic records.

19
20 (ii) California Department of Child Support Services: family electronic
21 records.

22
23 (iii) Office of a district attorney: criminal electronic records and juvenile
24 justice electronic records.

25
26 (iv) Office of a public defender: criminal electronic records and juvenile
27 justice electronic records.

28
29 (v) County department of probation: criminal electronic records, juvenile
30 justice electronic records, and child welfare electronic records.

31
32 (vi) Office of city attorney: criminal electronic records, juvenile justice
33 electronic records, and child welfare electronic records.

34
35 (vii) Office of county counsel: criminal electronic records, mental health
36 electronic records, child welfare electronic records, and probate
37 electronic records.

38
39 (viii) County child welfare agency: child welfare electronic records.

40
41 (ix) County public guardian: criminal electronic records, mental health
42 electronic records, and probate electronic records

43

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43

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

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

(xii) For good cause, a court may grant remote access to electronic records in particular case types to government entities beyond those listed in (b)(1)(i)-(xi). For purposes of this rule, “good cause” means that the government entity requires access to the electronic records in order to adequately perform its statutory duties or fulfill its responsibilities in litigation.

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

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

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

(c) Terms of remote access

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

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

1
2 **(d) Responsibilities of government entities**

3
4 (1) If a person is accessing electronic records on behalf of a government entity, the
5 government entity must approve granting access to that person, verify the
6 person's identity, and provide the court with all the information it needs to
7 authorize that person to have access to electronic records.

8
9 (2) If a person accessing electronic records on behalf of a government entity leaves
10 his or her position or for any other reason is no longer entitled to access, the
11 government entity must immediately notify the court so that it can terminate the
12 person's access.

13
14 **(e) Vendor contracts, statewide master agreements, and identity and access**
15 **management systems**

16
17 A court may enter into a contract with a vendor to provide identity verification,
18 identity management, or user access services. Alternatively, if a statewide identity
19 verification, identity management, or access management system or a statewide
20 master agreement for such systems is available, courts may use those to for identity
21 verification, identity management, and user access services.

22
23 **Rule 2.542. Security of confidential information**

24
25 **(a) Secure access and encryption required**

26
27 If any information in an electronic record that is confidential by law or sealed by
28 court order may lawfully be provided remotely to a government entity, any remote
29 access to the confidential information must be provided through a secure platform
30 and any electronic transmission of the information must be encrypted.

31
32 **(b) Vendor contracts and statewide master agreements**

33
34 A court may enter into a contract with a vendor to provide secure access and
35 encryption services. Alternatively, if a statewide master agreement is available for
36 secure access and encryption services, courts may use that master agreement.
37

1 **Rule 2.543. Audit trails**

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

4
5 The court must have the ability to generate an audit trail identifying when an
6 electronic record was remotely accessed, who remotely accessed the electronic
7 record, and under whose authority the user gained access to the electronic record.
8

9 **(b) Audit trails available to government entity**

10
11 (3) A court providing remote access to electronic records under this article must
12 make limited audit trails available to authorized users of the government entity.
13

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

18 **Rule 2.544. Additional conditions of access]**

19
20 To the extent consistent with these rules and other applicable law, a court must
21 impose reasonable conditions on remote access to preserve the integrity of its
22 records, prevent the unauthorized use of information, and protect itself from
23 liability. The court may choose to require each user to submit a signed, written
24 agreement enumerating those conditions before it permits that user to access
25 electronic records remotely. The agreements may define the terms of access,
26 provide for compliance audits, specify the scope of liability, and provide for
27 sanctions for misuse up to and including termination of remote access.
28

29 **Rule 2.545. Termination of remote access**

30
31 **(a) Remote access a privilege**

32
33 Remote access under this article is a privilege and not a right.
34

35 **(b) Termination by court**

36
37 A court that provides remote access may terminate the permission granted to any
38 person or entity eligible under the rules in article 4 to remotely access electronic
39 records at any time for any reason.
40
41

Monthly Project Monitoring Report

Report Period: 1/1/2018- 1/15/2018
Report Date:12/5/2017
Court Name: Placer
Prepared By: Greg Harding



JUDICIAL COUNCIL
OF CALIFORNIA
ADMINISTRATIVE DIVISION
INFORMATION TECHNOLOGY

Project Name	Placer County Hosting Center
Court Project Manager	Greg Harding
IBA Number	1033111
IBA Effective Date	11/1/2016
IBA End Date	4/30/2019
Project Start Date	October 2015
Estimated Finish Date	January 2018
Percent Complete	99%

1. Accomplishments / Plans

Accomplishments during *this Reporting Period*:

- San Benito Court Live

Plans during the *next Reporting Period*:

- Finalize IT Security Policy
- Final Accounting
- Final Project Report

2. Risks and Issues

Issue Status (Issues requiring resolution or others that may affect the proposed approach baseline):

- None.

Change Status (Considerations or new course of actions that change the proposed approach):

- None.

Risk Status (Report risks to the current approach, any risks discovered, and proposed risk responses):

- None.

3. Scheduled Milestones / Deliverables

List any Milestones that are late as well as Milestones due in the next 4 to 6 weeks (as applicable).

Milestone	Due Date (Actual)	Status
WBS 6 – Information Systems Framework and Security Policies Developed and Implemented	TBD	Final draft in review; central IT policies implemented; user restrictions pending

4. Payment Schedule and Milestones


List IBA payment milestones that have been completed, are yet to be completed, total IBA amount and payments remaining to be made.

IBA Installment Payments	IBA Installment Amount	IBA Payment Date	IBA Actual Payment
Court signs executed contracts with vendors	\$265,599.00		
Court develops all hardware and software specifications	\$470,901.00		
Total IBA Amount	\$736,500.00		
Remaining IBA Amount To Be Paid	\$736,500.00		
Project Tracking Milestones	Project Milestone Target Date	Project Milestone Actual Date	N/A For Project Milestone Tracking
WBS 1 – CCTC Requirements Document Completed	NOV 16	DEC 16	
WBS2 – Server Design	MAR17	FEB 17	
WBS3 – Server Build	APR17	APR17	
WBS4 – Network and Connectivity Design	JAN 17	JAN 17	


WBS5 – Network and Connectivity Implemented with connectivity to CCTC	MAY 17	JUNE 17	
WBS6 – Information Systems Framework and Security Policies Developed and Implemented	JUL17	AUG 17* Draft completed in August 17/ final adoption pending	
WBS7 – DMV Service Transition	JUL 17	AUG 17	
WBS7.1 – DMV DISA Approval	MAR 17	FEB 17	
WBS7.2 – DMV Connectivity Configured and implemented	JUN 17	APR17	
WBS9 – Interface rework completed	JUL 17	SEPT 17	
WBS10 – SJE Core Environments Created	MAY 17	MAY 17	
WBS11 – Initial SJE Data Copy	MAY 17	MAY 17	
WBS12 – Non-CMS Applications Installed	JUN 17	MAY 17	
WBS 13 – UAT of CCTC connectivity	SEPT 17	SEPT 17	
WBS14 –UAT of SJE and interfaces including DMV	AUG 17	AUG 17	
WBS15 – UAT of “managed court” services	SEPT 17	SEPT 17	
WBS 15.1 – Plumas/Sierra go-live plan created	AUG 17	AUG 17	
WBS 15.2 – Plumas/Sierra CMS hosting transition complete	OCT 17	SEPT 17	
WBS 15.3 – Plumas/Sierra Managed Court services transition complete	OCT 17	SEPT 17	
WBS 15.4 – Plumas/Sierra transition complete	OCT 17	SEPT 17	
WBS 16.1 Lake go live plan created	SEPT 17	SEPT 17	
WBS 16.2 Lake CMS hosting transition complete	NOV 17	DEC 17	
WBS 16.3 Lake Managed Court services transition complete	NOV 17	DEC17	
WBS 16.4 Lake transition complete	NOV 17	DEC 17	
WBS 17.1 Trinity go-live plan created	SEPT 17	OCT 17	
WBS 17.2 Trinity CMS hosting transition complete	OCT 17	OCT 17	
WBS 17.3 Trinity Managed Court services transition complete	NA	NA	
WBS 17.4 Trinity transition complete	OCT 17	OCT 17	
WBS 18.1 San Benito go-live plan created	OCT 17	DEC 17	
WBS 18.2 San Benito CMS hosting transition complete	DEC 17	JAN 18	
WBS 18.3 San Benito Managed Court services transition complete	DEC 17	JAN 18	
WBS 18.4 San Benito transition complete	DEC 17	JAN 18	

WBS 19.1 Modoc go-live plan created	NOV 17	DEC 17	
WBS 19.2 Modoc CMS hosting transition complete	JAN 18	DEC17	
WBS 19.3 Modoc Managed Court services transition complete	JAN 18	DEC 17	
WBS 19.2 Modoc transition complete	JAN 18	DEC 17	


Signature of authorized court representative

BY (Authorized Signature)  /s/ Jake Chatters
PRINTED NAME AND TITLE OF PERSON SIGNING Jake Chatters

Signature of authorized JC Information Technology Manager

BY (Authorized Signature) 
PRINTED NAME AND TITLE OF PERSON SIGNING

Signature of authorized JC Budget Services Director

BY (Authorized Signature) 
PRINTED NAME AND TITLE OF PERSON SIGNING